PK-yrityksen IT-infrastruktuuri

Kartoitus, analysointi, parannussuunnittelu ja toteutus

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietotekniikan koulutusohjelma

Riihimäki, kevät 2015

Jani Ekholm

Jani Ekholm

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

RIIHIMÄKI
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka

Tekijä Jani Ekholm **Vuosi** 2015

Työn nimi PK-yrityksen IT-infrastruktuuri

TIIVISTELMÄ

Tämän opinnäytetyön toimeksiantajana oli Tilitoimisto Markku Mäkelä Oy. Työn tarkoituksena oli kehittää, uudistaa ja modernisoida yrityksen IT-infrastruktuuri sekä laatia tietoturvasuunnitelma. Tavoitteena oli luoda prosessit ja toimintamallit, joilla yrityksen IT-ympäristöä voitiin hallita tehokkaasti ja turvallisesti.

Työn luonteen vuoksi projektissa tutkittiin lukuisia IT-infrastruktuurin rakenteita ja palvelimien palveluita. Lisäksi perehdyttiin ITIL-malliin, jossa IT-johtaminen tukeutuu prosesseihin. Lähdemateriaalina käytettiin alaan liittyviä julkaisuja ja kirjallisuutta sekä lukuisia www-sivustoja. Myös opinnäytetyön tekijän työkokemusta hyödynnettiin projektin toteutuksessa.

Teoriaosuuden tavoitteena oli selvittää parhaat tavat, menetelmät ja standardit, joilla laaja työ voitaisiin suorittaa. Tarkoituksena oli myös taata, että ympäristö tulisi vastaamaan nykypäivän vaatimuksia niin tietoturvan kuin käytönkin osalta.

Opinnäytetyön tuloksena toimeksiantajan IT-infrastruktuuri saatettiin vastaamaan nykypäivän standardeja ja yrityksen johto oppi hyödyntämään omaa ympäristöään lukuisilla uusilla tavoilla. Lisäksi työn myötä toimeksiantajalle luotiin ajantasainen standardia myötäilevä tietoturvasuunnitelma. Opinnäytetyön jälkeen yrityksellä oli käytössään ajantasainen, tietoturvallinen ja moderni IT-infrastruktuuri ja se vastaa taloushallintoliiton auktorisoidulle yritykselle asetettuihin vaatimuksiin.

Avainsanat **ITIL 2011, Palvelin, IT-infrastruktuuri, Windows, hallinta**

Sivut 54 s. + liitteet 31 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

RIIHIMÄKI
Degree Programme in Information technology
Data communications

Author Jani Ekholm **Year** 2015

Subject of Bachelor's thesis IT-infrastructure in an SME

ABSTRACT

This thesis was commissioned by Tilitoimisto Markku Mäkelä Oy. The purpose was to develop, renew and modernize the IT-infrastructure of the company and to create an information security plan. The goal was to create processes and functional models which would be used to safely and efficiently manage the IT-environment of the company.

During the project numerous server services and IT-infrastructure structures were studied because of the nature of the work. Also the ITIL-model, where the IT-management relies on processes, became familiar to the author of this thesis. Literature and publications as well as several web-based sources were used as reference material here. The author's knowledge and experience from his occupation were also utilized in the writing process of the thesis.

The aim of the theoretical part was to examine the best practices, techniques and standards which were used in the field to complete the large-scale project. An additional purpose was to ensure that the IT-environment would comply with the requirements today as to information security and usage.

As a result of the thesis, the commissioner's IT-infrastructure was developed to comply with the standards and the management staff of the company learnt to utilize their new environment in many different ways. An information security plan was also created by the standard. Upon the completion of the thesis, the client had an up to date, modern and secure environment, which complies with regulations set by FMA for authorized enterprises.

Keywords **ITIL 2011, Server, IT-infrastructure, Windows, Management**

Pages 54 p. + appendices 31 p.

AD - Active Directory. Windows-ympäristön palvelukokoelma.

AD DS - Active Directory Domain Services. Windows-toimialueen hakemistopalvelu ja käyttäjätietokanta.

ARP – Address Resolution Protocol. Selvittää IP-osoitetta vastaavaan MAC-osoitteen.

ATM - Asynchronous Transfer Mode. Asynkroninen tiedonsiirtotapa.

BIOS - Basic Input-Output System. Tietokoneohjelma, joka etsii ja lataa käyttöjärjestelmän keskusmuistiin sekä käynnistää sen tietokoneen käynnistyessä.

Canonical Name – resurssin tyyppi DNS:ssä.

CI – Configuration Item. Konfiguraatioyksikkö.

CMS – Content Management System. Sisällönhallintajärjestelmä.

CSMA/CS - Carrier Sense Multiple Access With Collision Detection. Varausmenetelmä tietoliikenteen siirtotiehen.

DC – Domain Controller. Toimialueen ohjauspalvelin.

DHCP - Dynamic Host Configuration Protocol. Verkkoprotokolla, jonka yleisin tehtävä on jakaa IP-osoitteita.

DNS - Domain Name System. Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.

Domain – AD:n toimialue. Verkko-objektien looginen ryhmä. Jakavat saman AD:n tietokannan.

Domain Naming Master – FSMO-rooli. Vastuussa forestin laajuisesta nimeämisestä.

DRP – Disaster Recovery Plan. Katastrofin hallintasuunnitelma.

EIGRP - Enhanced Interior Gateway Routing Protocol. Ciscon suljettu, kaupallinen reititysprotokolla.

Ethernet - pakettipohjainen lähiverkkoratkaisu.

Forest – AD:n Metsä. Kokoelma puita, joilla yhteinen globaali luettelo, hakemistorakenne, looginen rakenne ja hakemiston kokoonpano.

FQDN – Fully Qualified Domain Name. Täydellinen tietokoneen toimialueen nimi.

FSMO - Flexible Single Master Operations. Toimialueen ohjaimen joukko tehtäviä.

GE - Gigabit Ethernet. Termi kuvaamaan tiedonsiirron tekniikka.

GPO – Group Policy Object. Ryhmäkäytäntöobjekti.

ICMP – Internet Control Message Protocol. TCP/IP:n kontrolliprotokolla.

IEC - International Electrotechnical Commission. Kansainvälinen sähköalan standardointiorganisaatio.

IEEE - Institute of Electrical and Electronics Engineers. Kansainvälinen tekniikan alan järjestö.

IP - Internet Protocol. Protokolla TCP/IP-mallin internet-kerroksessa.

IPSec – IP Security Architecture. Salattu tietoliikenneprotokolla.

ISMS - Information Security Management System. Kokoelma käytäntöjä tietoturvaan ja IT:n riskeihin.

ISO - International Organization for Standardization. Kansainvälinen standardisoimisjärjestö.

IT - Informaatioteknologia. Tietojen käsittelyä tietokoneiden ja digitaalisen tietoliikenteen avulla.

ITIL - Information Technology Infrastructure Library. Kokoelma hallinnan ja johtamisen käytäntöjä IT-palveluihin.

LAN – Local Area Network. Lähiverkko. Rajatulla alueella toimiva tietoverkko.

LDAP – Hakemistopalvelun verkkoprotokolla. Käyttötarkoituksena autentikointi ja käyttöoikeuksien tarkastaminen.

LLC – Logical Link Control. OSI-mallin toisen ja kolmannen kerroksen välissä oleva alikerros.

LSASS - Local Security Authority Subsystem Service. Windowsin prosessi, joka vastaa turvallisuudesta järjestelmässä.

MAC – Media Access Control. Verkkosovittimen yksilöivä osoite Ethernet-verkossa.

NAT – Network Address Translate. Kääntää julkisen IP:n yksityiseksi tai päinvastoin.

NetFlow – Tapa, jolla kerätään tietoja IP-liikenteestä kun se lähtee tai saapuu laitteelle.

NTFS - New Technology File System. Tiedostojärjestelmä.

OSI-malli - Open Systems Interconnection Reference Model. Kuvaus tiedonsiirtoprotokollien yhdistelmästä seitsemässä kerroksessa.

OSPF - Open Shortest Path First. Avoimiin standardeihin perustuva organisaation sisäinen TCP/IP-verkkojen reititysprotokolla.

OU – Organization Unit, organisaatioyksikkö. Käytetään muodostamaan toimialueelle loogisesti hallittava rakenne. Sijoitetaan käyttäjiä ja koneita.

PDC – Primary Domain Controller. Ylin toimialueen ohjauspalvelin.

PTR – Pointer Record. Canonical Namen osoitin.

PXE - Preboot Execution Environment. Käynnistää verkosta noudettavan ohjelmistokokoonpanon.

RDP - Remote Desktop Protocol. Protokolla, jonka avulla saadaan graafinen käyttöliittymä yhdistettäessä verkon yli toiseen laitteeseen.

RFC – Request for Change. Muutospyyntö. Virallinen ehdotus jonkin muutoksen teosta.

RID – Relative ID. Vaihtelevan mittainen numero, joka annetaan objektille sen luonnissa.

SaaS – Software as a Service. Ohjelmiston hankkiminen palveluna.

Schema - Active Directoryn komponentti, joka määrittelee kaikki kohteet ja määritteet, joita hakemistopalvelu käyttää tiedon tallentamiseen.

Schema Master – FSMO rooli. Hallinnoi schemaa.

SID – Security Identifier. Yksilöllinen ja muuttumaton tunniste objektille.

Site – Verkon topologian tai fyysisen rakenteen kuvaamista AD DS:ssä.

SKMS – Service Knowledge Management System. Kokoelma työkaluja ja tietoa informaation hallintaan.

Skripti – Komentosarja tehtävien automatisointiin.

SNAP – Subnetwork Access protocol. LLC:n laajennus.

SNMP – Simple Network Management Protocol. TCP/IP-verkkojen hallinnassa käytettävä tietoliikenneprotokolla.

SQL - Structured Query Language. Kyselykieli, jolla relaatiotietokantaan voi tehdä erilaisia hakuja, muutoksia ja lisäyksiä.

SSH – Secure Shell. Salattu tietoliikenteen protokolla.

TAL - Taloushallintoliitto

TCP – Transmission Control Protocol. Usean Internet-liikennöinnissä käytettävän tietoverkkoprotokollan yhdistelmä.

UPS - Uninterruptible Power Supply. Varavirtalaite.

WAN – Wide Area Network. Laajaverkko. Kattaa laajoja maantieteellisiä alueita.

WLAN – Wireless Local Area Network. Langaton lähiverkkotekniikka.

VLAN – Virtual LAN. Virtuaalilähiverkko. Tekniikka, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisiin osiin.

WMI – Windows Management Instrumentation. Kerää laite- ja käyttäjätietoja.

VPN – Virtual Private Network. Menetelmä, jolla julkisen verkon yli yhdistetään verkkoja.

SISÄLLYS

1 JOHDANTO

Opinnäytetyö toteutettiin Tilitoimisto Markku Mäkelä Oy:lle. Kyseessä on Hämeenlinnassa vuonna 1987 perustettu taloushallinnon palveluja tarjoava yritys, jonka palveluksessa on 12 päätoimista kirjanpitäjää. Tilitoimisto Markku Mäkelä Oy:n tarjoamia palveluja ovat kirjanpito tilinpäätöksineen ja veroilmoituksineen, osto- ja myyntireskontrapalvelut, palkanlaskenta, asiakaslaskutus, asiakkaiden maksuliikenteen hoitaminen ja erilaiset asiantuntijapalvelut. Asiakasyrityksiä tilitoimistolla on noin 250, joista 30 on asunto-osakeyhtiöitä tai kiinteistöosakeyhtiöitä ja 220 osakeyhtiöitä, kommandiittiyhtiöitä tai toiminimiä. Tilitoimiston asiakkaat toimivat Hämeenlinnan seudulla hyvin erilaisilla toimialoilla. Suurimmat yritykset ovat rakennusliikkeitä (38 yritystä), putkiasennusliikkeitä (3 kpl) ja sähköasennusliikkeitä (4 kpl). Pääsääntöisesti yritykset ovat pieniä ja työllistävät keskimäärin 3 henkilöä/yritys.

Pysyäkseen menestyvänä yrityksenä Tilitoimisto Markku Mäkelä Oy on panostanut kehitykseen, koulutukseen ja laatuun. Vuonna 2005 yritys hyväksyttiin Suomen Taloushallintoliitto ry:n jäseneksi ja keväällä 2005 Tiliinstituuttisäätiön KLT-lautakunta myönsi yritykselle auktorisoinnin. Tiliinstituuttisäätiö valvoo auktorisoitujen tilitoimistojen toimintaa mm. toimistotarkastuksilla, minkä johdosta yrityksen on jatkuvasti panostettava toimintaansa pysyäkseen menestyvänä ja luotettavana taloushallintopalvelujen tarjoajana.

1.1 Lähtökohta

Opinnäytetyö tehtiin projektina yritykselle. Yrityksestä ehdotettiin heidän IT-ympäristönsä kartoitusta ja analysointia, minkä pohjalta tuli tehdä suunnitelmat päivityksistä ja parannuksista sekä toteuttaa ne. Projektin tarkoituksena oli tuottaa yritykselle nykypäivän standardeja ja vaatimuksia vastaava ympäristö laitteineen, ohjelmistoineen ja palveluineen sekä luoda puuttuva tietoturvasuunnitelma. Lisäksi ympäristöstä tarvittiin selkeä dokumentaatio siitä, mitä ympäristöstä löytyy ja miten kaikki on konfiguroitu ja määritelty.

Yrityksen toimistopäällikön mukaan ympäristö on jokseenkin sekava ja aikaansa jäljessä. Lisäksi tarpeen päivityksille luovat kolmansien osapuolien järjestelmät ja ohjelmistot. (Liite 1.)

Projekti kattoi yrityksen koko IT-infrastruktuurin kartoituksen, analysoinnin, parannussuunnitelmat ja toteutuksen hyväksikäyttäen ITIL:iä (2011) sekä Microsoftin sertifiointidokumentteja ja Best Practices -menetelmiä. Myös Microsoftin Technet -www-sivuja hyödynnettiin. Lisäksi tiettyihin asioihin otettiin huomioon ISO17799/ISO27002 standardin viitteitä.

1.2 Tavoitteet

Tavoitteena oli toteuttaa yritykselle nykypäivän standardeihin ja menetelmiin perustuva IT-infrastruktuuri ja dokumentoida se. Ympäristö käsittää pääsääntöisesti palvelimet, työasemat, verkkolaitteet ja tulostimet. Tavoitteena oli, että toimeksiantajalle luodaan kustannustehokas ratkaisu, joka palvelisi sitä laitteiden ja ratkaisuiden elinkaaren ajan mahdollisimman vaivattomalla ylläpidolla, koska yritys halusi itse ylläpitää ympäristöään. Tästä johtuen opinnäytetyö lopulta laajeni myös muutamien henkilöiden kohdalla ympäristön hallitsemisen kouluttamiseen.(Liite 2.)

Yrityksen johdon tavoitteena oli oppia tuntemaan paremmin oma ympäristönsä sekä siihen vaikuttavat tekijät ja niiden hallinnointi. Lisäksi suurena tavoitteena oli tietoturvasuunnitelman laatiminen ja sen täytäntöönpano.

1.3 Menetelmät

Tavoitteiden saavuttamiseksi projekti jaettiin viiteen päävaiheeseen, joihin hyväksikäytettiin eri keinoja lopputuloksen saavuttamiseksi. Ympäristön kartoitus toteutettiin vierailemalla yrityksen tiloissa muutaman päivän ajan, jolloin tietoa kerättiin eri laitteista ja järjestelmistä. Kartoituksen pohjalta tehtiin analyysi siitä, mitä muutoksia ympäristö tarvitsee.

Kun ympäristön tarpeet oli selvitetty sekä keskusteltu niistä toimeksiantajan kanssa, luotiin suunnitelma muutoksille. Suunnitelman valmistumisen jälkeen sovittiin toimeksiantajalle sopiva ajankohta, jolloin muutokset vietäisiin tuotantoympäristöön. Näin muodostui testaus ja lopullinen toteutus.

2 TEORIA

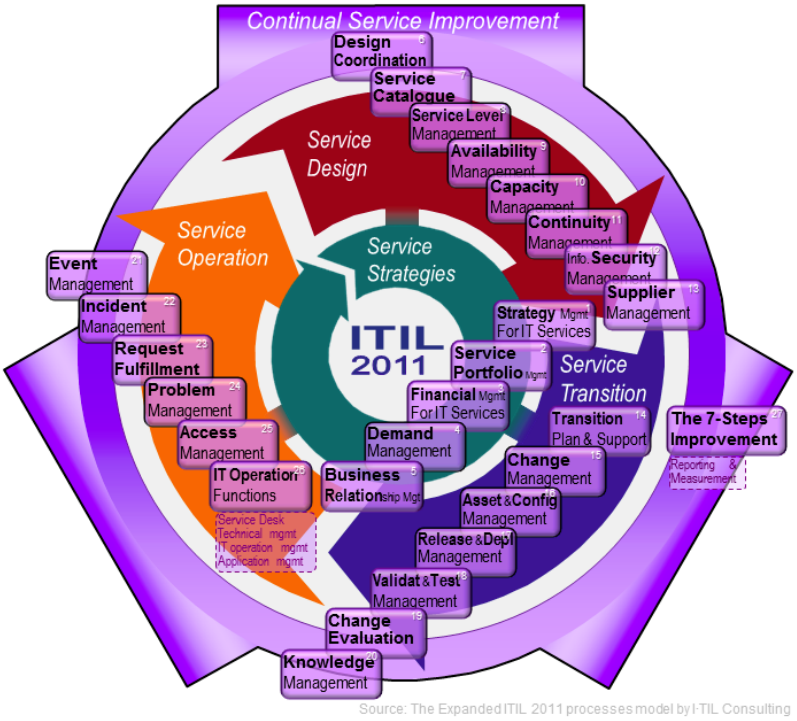
Työssä käytetyt menetelmät perustuvat eri teorioihin, standardeihin ja Best Practices -malleihin. Nykypäivänä IT-infrastruktuurin hallintaan ja muutoksiin sovelletaan pääsääntöisesti ITIL-käytäntöjä. Opinnäytetyön projektiluontoisuuden vuoksi työssä käytettiin ITIL-mallin osia kolmesta ensimmäisestä kirjasta. Ne määrittävät miten strategia ja muutoshallinta vaikuttavat koko projektin läpiviemiseen ja näin ollen ne toimivat pääsääntöisenä prosessirunkona koko työlle.

Teknisen toteutuksen osalta lähteenä käytettiin pääsääntöisesti Microsoftin parhaita menetelmiä ja dokumentointia. Tältä osin teoriassa käsitellään vain projektissa esiintyviä aiheita ja menetelmiä päällisin puolin ja rajataan kaikki muu ulkopuolelle.

2.1 ITIL 2011

ITIL (Information Technology Infrastructure Library) on IT-palveluiden hallintaan ja johtamiseen koottu kokoelma käytäntöjä. Se on prosessikehys, joka on globaalisti tunnustettu ja se soveltuu niin isojen kuin pientenkin yritysten IT-prosessikehykseksi. Periaatteena on IT-palveluiden johtaminen tukeutuen prosesseihin. Se sisältää viisi eri osiota (Kuva 1):

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement.



Kuva 1. ITIL 2011 -malli

Näistä Service Strategy, Service Design ja Service Transition olivat keskeisessä osassa tässä työssä. Yllä mainituista kolmesta osiosta ei kuitenkaan käytetty kaikkea mahdollista vaan rajaus tehtiin niihin asioihin jotka työtä hyödyttivät ja siihen eniten vaikuttivat.

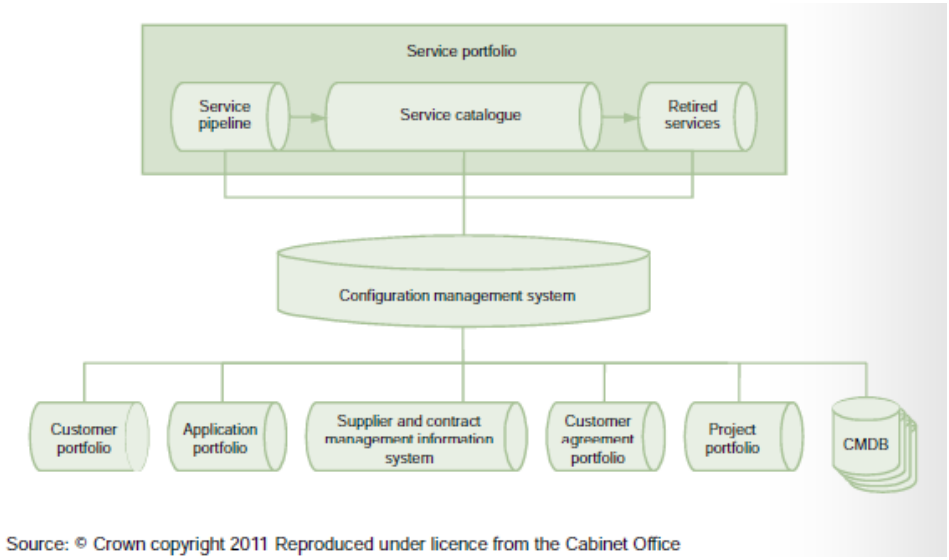
2.1.1 Service Strategy

Service Strategy -osion tarkoituksena on määrittää palveluiden elinkaaren näkökulma, suunnitelmat, malli ja asetelma, jotka palveluntarjoaja tarvitsee toteuttaakseen ympäristön vastaamaan organisaation liiketoiminnan tuloksia. Se on lähtökohtana organisaation toiminnalle, jonka suunnittelua tarkastellaan ulkopuolisen näkökulmasta. Vaiheessa mietitään mitä palveluita tuotetaan ja mitkä ovat asiakkaan tarpeet. Oleellista on myös asiakkaan omat resurssit sekä tarve ulkoistaa tai tehdä itse. Service Strategy -osan myötä tulee myös liiketoiminnan kannalta määrittää palvelujen arvo sekä määrittää miten ne tuotetaan. Huomattavaa on, että ITIL:n mukaan ei osteta palveluita, vaan ratkaisuja tarpeisiin. (Wakaru 2012.)

Tämä vaihe voidaan jakaa kolmeen prosessiin:

- Business Relationship management
- Service Portfolio Management
- Financial Management for IT Services.

Keskeisenä osana vaihetta on Service Portfolio Management (Kuva 2), jonka tarkoituksena on liiketoiminnan näkökulmasta kuvata tuotettavia palveluita.



Kuva 2. Service Portfolio

Service Portfolion tarkoituksena on havainnollistaa palveluntarjoajan tekemiä investointeja ja sitoumuksia kaikille asiakkaille ja markkinoille. Se esittää kehitteillä ja tuotannossa olevia sekä jo elinkaaren lopussa olevia palveluita. Näistä tuotannossa olevat ja elinkaaren lopussa olevat palvelut sijaitsevat Service Cataloguessa ja näin näkyvät asiakkaille. Service Pipelinessä sijaitsevat kehitteillä olevat palvelut eivät näy asiakkaille. (Wakaru 2012.)

Työssä ei varsinaisesti oteta kantaa Service Strategy -vaiheen prosesseihin, koska toimeksiantajalla ei ole IT-palveluiden tarjoajaa eikä yritys tarjoa IT-palveluita. Toisaalta opinnäytetyön tekijä toimii periaatteessa palveluiden tarjoajana ja näin ollen Service Portfolion muodostus otettiin mukaan soveltaen.

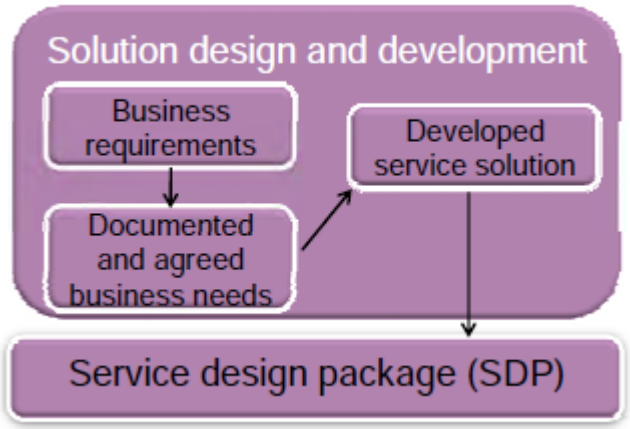
2.1.2 Service Design

Service Design -vaiheen tarkoituksena on määrittää elinkaaren ajalle vaatimukset, joiden myötä IT-palvelun suunnitteluun asettuvat liiketoiminnan tavoitteet. Suunnittelussa on huomioitava:

- Palveluratkaisuiden suunnittelu (toiminnallinen, operatiivinen, hallintavaatimukset, palvelutason vaatimukset ja resurssit)
- Palvelunhallinnan järjestelmien ja välineiden suunnittelu, erityisesti Service Portfolion hallinta palveluiden elinkaaren läpi
- Teknologia- ja hallinta-arkkitehtuurin suunnittelu

– Prosessit, roolit, vastuut
– Palvelutasojen mittareiden suunnittelu.

Service Design -vaiheen tuloksena on Service Design Package (SDP) (Kuva 3), joka määrittää tarvittavat resurssit koko palvelun elinkaaren ajaksi. (Wakaru 2012.)



Kuva 3. Solution Design and Development

Service Design Package tulisi tuottaa aina Service Design -vaiheessa jokaiselle uudelle palvelulle. Myös palvelun suuren muutoksen ja poiston tulisi tuottaa SDP.
(Wakaru 2012.)

Itse Service Design -vaihe jakaantuu seuraaviin prosesseihin:
– Design Coordination
– Service Catalogue Management
– Service Level Management
– Availability Management
– Capacity Management
– IT Service Continuity Management
– Information Security Management
– Supplier Management.

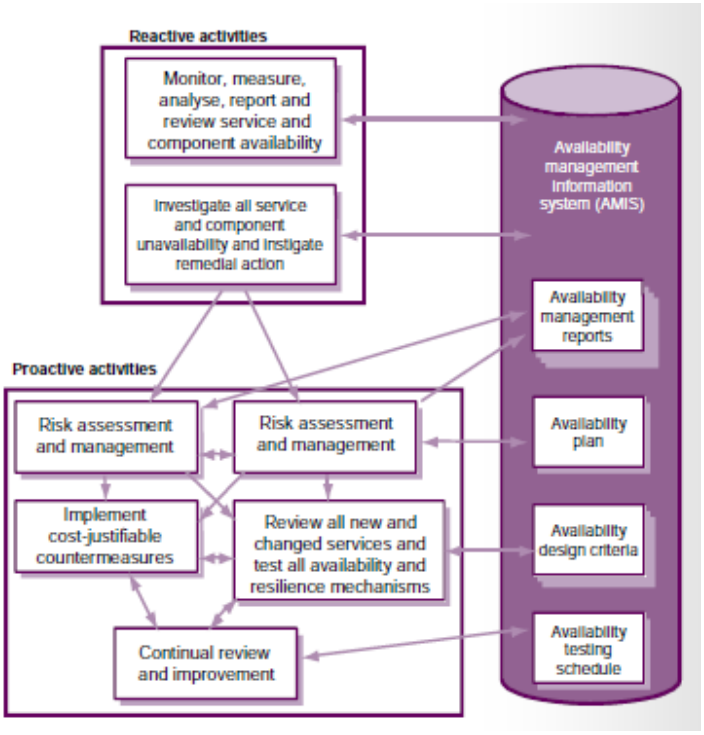
(Wakaru 2012.)

Näistä opinnäytetyöhön otettiin lähempään tarkasteluun mukaan Availability Management ja Information Security Management.

Availability Management määrittää jonkin palvelun, osan tai konfigurointikohteen kyvyn, joka yleensä mitataan ja ilmoitetaan prosentteina. Sen tarkoituksena on varmistaa, että toimitetut IT-palvelut saavuttavat tietyn sovitun palvelutason kustannustehokkaasti ja oikea-aikaisesti. Saatavuuden hallinnassa tarkastellaan kahta asiaa, palveluiden saatavuutta ja komponenttien saatavuutta. Siinä on kaksi pääelementtiä, reaktiiviset aktiviteetit ja proaktiiviset aktiviteetit (Kuva 4):

– Reaktiivisiin aktiviteetteihin kuuluvat monitorointi, mittarit, analysoinnit ja hallinta. Suorittavina eliminä ovat operatiiviset roolit.

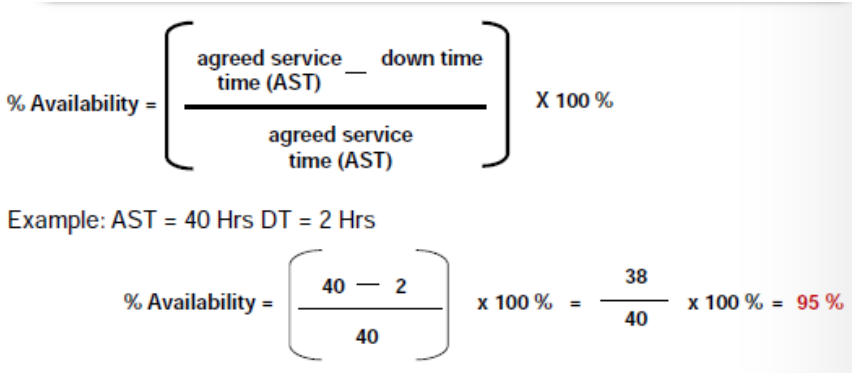
– Proaktiivisiin aktiviteetteihin kuuluvat suunnittelu, mallinnukset ja saatavuuden kehittäminen. Nämä ovat yleensä suunnitteluroolien tehtäviä. (Wakaru 2012.)



Kuva 4. Availability Management -prosessin aktiviteetit

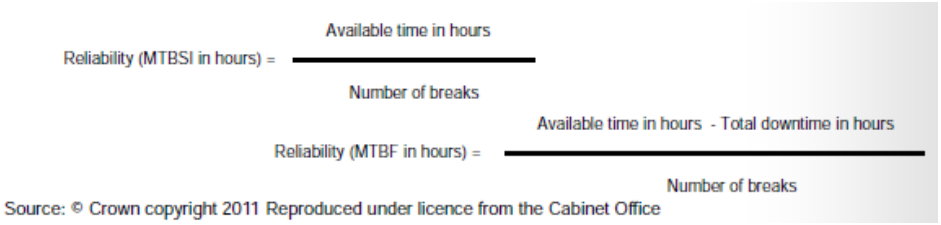
Peruskonseptiin kuuluu kuusi kohtaa:
– Service Availability
– Component Availability
– Reliability
– Maintainability
– Service Ability
– Vital Business Functions.

Palvelun saatavuus määrittää kaikki osa-alueet palvelun käytettävyyden ja ei-käytettävyyden osalta. Se määrittää myös komponentin käytettävyyden tai potentiaalisen vaikutuksen palvelun saatavuuteen komponentin ei-käytettävyyden osalta (Kuva 5). (Wakaru 2012.)



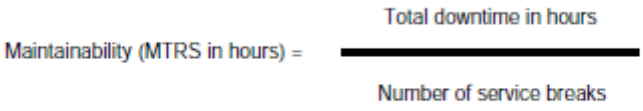
Kuva 5. Saatavuuden laskentakaava

Luotettavuudella mitataan sitä, kuinka pitkään jokin palvelu, komponentti tai konfiguraatiokohde voi toimia ilman häiriötä. Se yleensä mitataan ja raportoidaan kahdella eri tavalla: poikkeamien välinen aika (MTBSI) (kuva 6) tai häiriöiden välinen aika (MTBF) (Kuva 7). (Wakaru 2012.)



Kuva 6. Luotettavuuden laskentakaava

Huollettavuudella mitataan kuinka nopeasti jokin komponentti, palvelu tai konfiguraatiokohde voidaan palauttaa normaaliksi häiriön jälkeen. Se mitataan ja ilmoitetaan kuinka paljon aikaa kuluu palauttaa kohde normaaliksi (MTRS) (Kuva 7). (Wakaru 2012.)



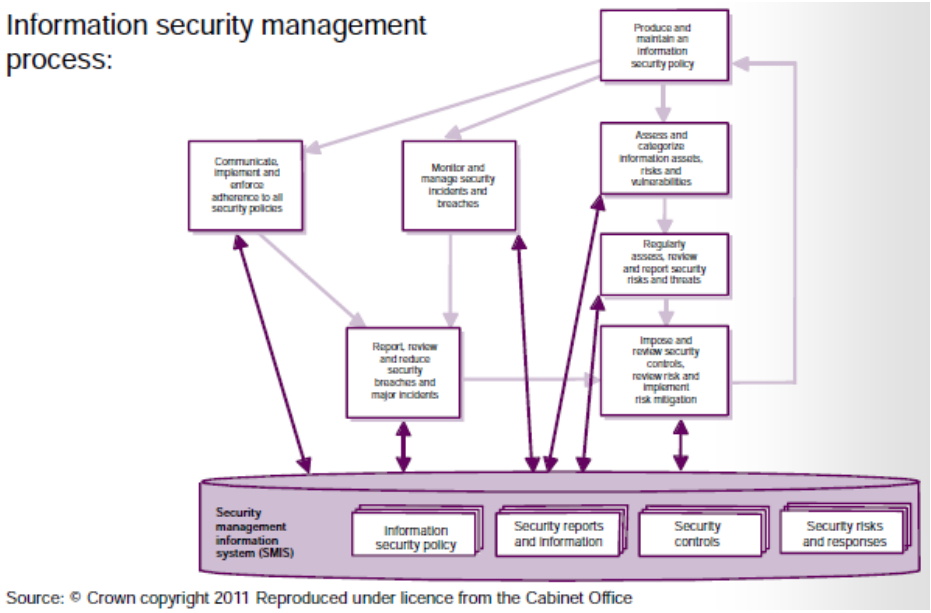
Kuva 7. Huollettavuuden laskentakaava

Tilanteessa, jossa vuorokauden ympäri toimiva palvelu on ollut 6000 tuntia käytössä ja sinä aikana on ollut kaksi käyttökatkoa, toinen kolmen tunnin mittainen ja toinen yhdentoista tunnin mittainen, perustuen saatavuuden, kahden eri luotettavuuden ja huollettavuuden mittaamiseen, voidaan luoda seuraavat esimerkkilaskelmat:

Taulukko 1. Esimerkki mittareiden laskemisesta

Availability	= (6000-(3+11))/6000*100	= 99,77%
Reliability MTBSI	= 6000/2	= 3000 tuntia
Reliability MTBF	= 6000-(3+11)/2	= 2993 tuntia
Maintainability MTRS	= (3+11)/2	= 7 tuntia

Information Security Managementin päätarkoituksena on yhdenmukaistaa IT:n turvallisuus liiketoiminnan turvallisuuden kanssa. Se myös varmistaa, että luottamuksellisuus ja eheys sekä organisaation omaisuuden, informaation ja IT-palveluiden saatavuus vastaavat liiketoiminnan tarpeita. Tietoturvan hallinnan tavoitteena on suojautua luottamuksen, eheyden ja saatavuuden virheistä johtuvilta haitoilta. Nämä voivat vaikuttaa järjestelmiin, jotka toimittavat tietoa tai niihin, jotka tietoa käyttävät (Kuva 8). (Wakaru 2012.)



Kuva 8. Information Security Management -prosessi

Tarkemmin määriteltynä turvallisuuden tavoitteena on varmistaa että:

- Tiedot ovat täydellisiä, tarkkoja ja suojattu luvattomalta muutokselta (eheys)
- Tietoja ovat tarkkailleet ja luovuttaneet vain ne, joilla on siihen oikeus (luottamuksellisuus)
- Tiedot ovat saatavissa ja käytettävissä tarvittaessa ja että järjestelmät, jotka jakavat tietoa, voivat vastustaa hyökkäyksiltä ja palautua tai estää vikatilanteita (saatavuus)
- Liiketoiminta sekä tietojen vaihto henkilöiden, kumppaneiden ja yritysten välillä on luotettavaa (aitous) (Wakaru 2012.).

Turvallisuuden hallinnan tulisi olla keskipiste kaikissa IT-turvallisuuden asioissa. Sen täytyy taata, että tietoturvapolitiikka laaditaan, ylläpidetään ja jalkautetaan kattamaan IT-järjestelmien ja -palveluiden käyttöä ja sen tärkeimpinä alueina tulisi olla luottamuksellisuus, eheys ja saatavuus liiketoiminnan puitteissa. (Wakaru 2012.)

Turvallisuuspolitiikalla tulisi olla täysi tuki tietohallinnon ja liiketoiminnan ylimmältä johdolta. Sen tulisi kattaa kaikki turvallisuuteen liittyvät seikat, olla tarkoituksenmukainen, vastata liiketoiminnan tarpeisiin ja sisältää seuraavat asiat:

- Yleinen tietoturvakäytäntö
- IT-laitteiden käyttö
- Käyttövaltuushallinta
- Salasanakäytäntö
- Sähköpostikäytäntö
- Internetin käyttö
- Virustorjunnan käytäntö
- Tiedon luokituksen käytäntö
- Dokumentin luokituksen käytäntö
- Etäkäytön käytäntö

- Käytäntö toimittajien pääsyyn IT-palveluihin, tietoihin ja komponentteihin
- Käytäntö sähköisen aineiston tekijänoikeusrikkomuksiin
- Hävitys- ja poistokäytäntö
- Käytäntö tietojen säilytykseen.

Kyseisten käytäntöjen tulisi olla kaikkien saatavilla. (Wakaru 2012.)

Tietoturvapolitiikkaa käsitellään tarkemmin kappaleessa 2.4. Osiossa tarkastellaan ISO 17799:2005 / ISO 27002:2005 standardia, jonka perusteella luodaan tietoturvasuunnitelma.

2.1.3 Service Transition

Service Transition on suunnittelun jälkeinen vaihe, jota käytetään päivittäisessä toiminnassa siirtymävaiheessa ja käyttöönottovaiheessa. Sen avulla pyritään suorittamaan mutkaton käyttöönotto sovittujen aikataulujen, kustannusten ja vaatimusten puitteissa sekä minimoimaan muutosten vaikutus liiketoimintaan. Service Transition -vaiheessa tulisi myös perustaa konfiguraatiotietokanta (CMS), mikäli sellaista ei vielä ole. CMS:n ollessa jo käytössä, tulisi se päivittää. Kyseinen kuvaus organisaation sovelluksista, palveluista ja laitteista on todella arvokas.
Service Transiotion -vaihe jakaantuu seuraaviin prosesseihin:

- Transition Planning and Support
- Change Management
- Service Asset and Configuration Management
- Release and Deployment Management
- Knowledge Management. (Wakaru 2012.)

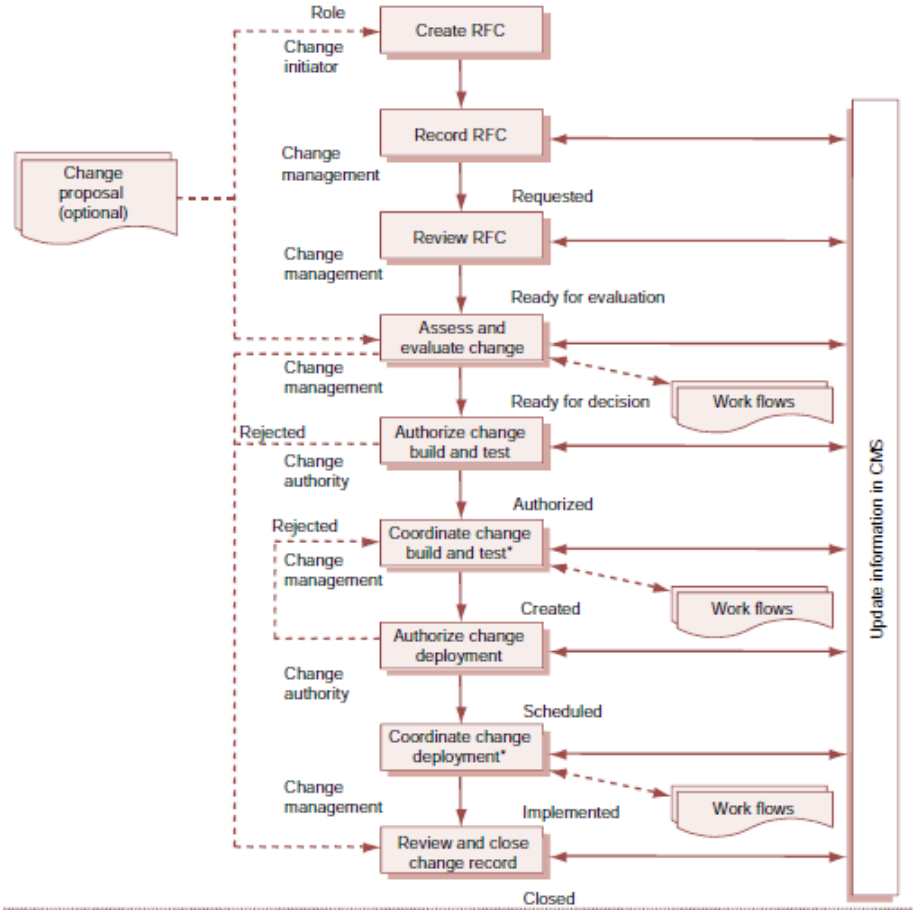
Tästä vaiheesta työhön suurelta osin vaikutti Change Management. Lisäksi tarkasteluun otettiin mukaan Release and Deploy Management sekä osittain Service Asset and Configuration Management.

Muutoshallinta (Change Management)
Muutospyyntö, RFC, on virallinen ehdotus jonkin muutoksen teosta. Se sisältää tiedot muutoksesta ja voi olla joko paperimuotoisena tai sähköisenä. Muutos on jonkin asian lisäys, modifikaatio tai poisto, joka voi vaikuttaa IT-palveluun. Soveltamisalueena ovat muutokset kaikkiin arkkitehtuureihin, prosesseihin, työkaluihin, mittareihin ja asiakirjoihin, sekä IT-palveluihin ja konfiguraatiomäärityksiin. (Wakaru 2012.)

Muutoshallinnan tarkoituksena on kontrolloida elinkaaren ajan muutoksia mahdollisimman pienellä vaikutuksella IT-palveluihin. Tavoitteena on vastata asiakkaan liiketoiminnan muuttuviin vaatimuksiin maksimoiden sen arvo sekä vähentää poikkeamia ja häiriöitä. Tarkoituksena on myös varmistaa muutosten kirjaus ja arviointi ja että hyväksytyt muutokset priorisoidaan, suunnitellaan, testataan, toteutetaan, dokumentoidaan ja tarkastetaan kontrolloidulla tavalla. (Wakaru 2012.)

Muutoshallinnan laajuus kattaa koko palvelun elinkaaren ajan muutokset kaikkiin konfiguraatiomäärityksiin riippumatta siitä, ovatko ne fyysisiä laitteita, virtuaalisia tai sopimuksia. Se käsittää myös Service Design -vaiheen ratkaisut uusiin tai muuttuneisiin palveluihin, teknologia- ja hallinnointiarkkitehtuurit, prosessit palveluiden suunniteluun, siirtoon, operointiin ja kehittämiseen sekä mitattavien kohteiden mittareiden järjestelmiin ja metodeihin. (Wakaru 2012.)

Muutoksia on kolmenlaisia, normaali muutos, standardi muutos ja kiireellinen muutos. Normaali muutos on mikä tahansa muutos, joka ei ole standardi tai kiireellinen muutos. Se seuraa normaalin muutoksen prosessia (Kuva 9).



Kuva 9. Normaalin muutoksen prosessi

Standardi muutos on hyvin tunnettu ja dokumentoitu. Sillä on määritelty asia, joka laukaisee tarpeen prosessille. Yleensä lupa muutokselle on annettu etukäteen ja sillä on pieni riski kokonaisuuden vaikutukseen. Kuvasta 10 voidaan esimerkkinä ottaa uuden käyttäjätunnuksen luominen. Se sijoittuu elinkaaressa Service Operations -vaiheeseen ja sen prosessi on dokumentoitu suorittamista varten. (Wakaru 2012.)

Types of request	Documented work procedures	Lifecycle SS	SD	ST	SO	CSI
Request for change to service portfolios ⇥ New portfolio line item ⇥ To predicted scope, business case, baseline ⇥ Service pipeline	✓ Service change management	X				
Request for change to service or service definition ⇥ To existing or planned service attributes ⇥ Project change that impacts service design, for example, forecasted warranties ⇥ Service improvement	✓ Service change management	X	X	X	X	X
Project change proposal ⇥ Business change ⇥ No impact on service or design baseline	✓ Project change management		X	X		X
User access request	✓ User access procedure				X	
Operational activity ⇥ Tuning (within specification/ constraints) ⇥ Reboot hardware on failure if no impact on other services ⇥ Planned maintenance	✓ Local procedure, often pre-authorized				X	

Source: © Crown copyright 2011 Reproduced under licence from the Cabinet Office

Kuva 10. Esimerkki muutoksista ja niiden sijoittuminen elinkaarelle

Hätämuutokset kulkevat Change Advisory Board tai Emergency Change Advisory Board -elimen kautta, jossa muutoksen prosessi jaetaan asiaankuuluville teknisille ryhmille rakentamisen, testauksen ja toteutuksen perusteella. (Wakaru 2012.)

Julkaisu ja käyttöönottohallinta (Release and Deploy Management)

Prosessin tarkoituksena on tuottaa liiketoiminnan kannalta tarvittava uusi funktionaalisuus. Prosessin vaiheina ovat suunnittelu, aikataulutus ja kontrollointi palvelun rakentamiseen, testaukseen ja käyttöönottoon. Tavoitteena on määrittää ja sopia käyttöönottosuunnitelmat asiakkaiden ja omistajien kanssa. Päämääränä on myös uusien julkaisuiden luonti ja testaus sekä varmistaa uusien ja muutettujen palveluiden hyödyllisyys ja takuu. Liiketoiminnan näkökulmasta tärkeänä seikkana voidaan pitää tiedon siirtämistä asiakkaille ja käyttäjille, jotta uudesta palvelusta saa kaiken hyödyn irti. (Wakaru 2012.)

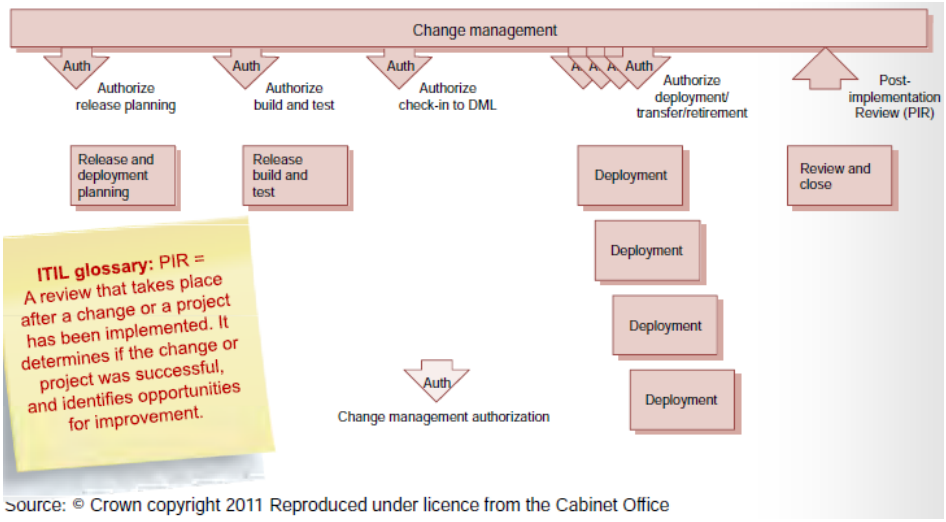
Prosessin sisältöön kuuluu paketoinnin, kokoamisen, testauksen sekä käyttöönoton järjestelmät ja toiminnot. Osana on myös Service Design -paketin palvelun muodostaminen ja sen luovuttaminen eteenpäin operatiiviselle taholle. Prosessi ei vastaa muutosten hyväksynnästä ja tarvitsee muutoshallinnan hyväksynnän palvelun käyttöönotoissa elinkaaren eri vaiheissa.

Julkaisun ja käyttöönoton hallintaan sisältyy tarvittavat konfiguraatiomääritykset julkaisuiden toteuttamiseksi, kuten:

- Fyysinen omaisuus kuten palvelimet ja verkot
- Virtuaalinen omaisuus kuten virtuaalipalvelin tai virtuaalinen varastointi
- Sovellukset ja ohjelmat
- Käyttäjien ja IT-henkilöstön koulutus
- Palvelut, mukaan lukien sopimukset.

(Wakaru 2012.)

Prosessin laajuus on nelivaiheinen (Kuva 11). Ensimmäinen vaihe käsittää suunnitelmat siitä, miten jokin julkaisu tehdään ja otetaan käyttöön. Toisessa vaiheessa julkaisu paketoidaan ja testataan. Kolmannessa vaiheessa julkaisu otetaan käyttöön. Vaihe voi olla moniosainen riippuen siitä, miten käyttöönotto halutaan tehdä. Neljännessä vaiheessa kerätään kokemukset ja palaute sekä tulostavoitteet ja saavutukset tarkastellaan uudelleen ja niistä otetaan opiksi. (Wakaru 2012.)



Kuva 11. Käyttöönoton vaiheet

Uusi julkaisu voidaan jakaa usealla tapaa moneen paikkaan, kuten esimerkiksi kaikki kerralla (Big-bang) tai vaiheittain. Julkaisu voi olla automatisoitu tai se joudutaan manuaalisesti ottamaan käyttöön. Tärkeää kuitenkin on, että julkaisun tiedot tallennetaan CMS-järjestelmään. (Wakaru 2012.)

Palveluomaisuuden ja konfiguraation hallinta (Service Asset and Configuration Management)

Tarkoituksena on palveluiden tuottamiseen tarvittavan omaisuuden kontrollointi, omaisuuden tarkka ja luotettava informaatio, joka sisältää kaikkien laitteiden ja konfiguraatioiden tiedot sekä relaatiot. Tavoitteena on taata, että IT-organisaation kontrollissa olevat asiat on tunnistettu, kontrolloitu ja ylläpidetty elinkaaren ajan. Myös laitteiden ja konfiguraatioiden tunnistus, hallinta, merkitseminen, raportointi, auditointi ja palveluiden varmistus sekä muut konfiguraation kohteet (CI), kuten versiot, määritelmät ja osatekijät sekä niiden ominaisuudet ja suhteet, ovat vaiheelle ominaisia seikkoja. Tiedot kirjataan Configuration Management System (CMS) -järjestelmään, jolla voidaan ylläpitää tarkkaa määritystä historiasta, suunnitelmista ja nykyisestä tilasta. (Wakaru 2012.)

CMS on kokoelma työkaluja, tietoja ja informaatiota, jota käytetään tukemaan Service Asset and Configuration Management -prosessia. CMS on osa laajempaa SKMS-järjestelmää ja se sisältää työkalut konfiguraatioiden määritysten ja niiden välisten relaatioiden tietojen keräämiseksi, varastoimiseksi, ylläpitämiseksi, päivittämiseksi, analysoimiseksi ja esittämiseksi. (Wakaru 2012.)

2.2 Lähiverkko

LAN (Local Area Network) on nopea tietoverkko, joka kattaa suhteellisen pienen maantieteellisen alueen. Tällainen voi olla esimerkiksi yhden talon koneiden muodostama tietokoneverkko tai yksittäisen yrityksen yhden toimipisteen verkko. Se yhdistää tyypillisesti työasemat, henkilökohtaiset tietokoneet, tulostimet, palvelimet ja muut laitteet. Lähiverkot tarjoavat tietokoneen käyttäjille monia etuja, kuten yhteisen pääsyn laitteisiin ja sovelluksiin, tiedostojen jaon lähiverkossa ja käyttäjien välisen kommunikaation joko sähköpostin välityksellä tai jollain muulla sähköisellä sovelluksella. (Cisco 2012.)

Tiedonsiirron nopeus lähiverkoissa on yleensä 10–1 000 megabittiä sekunnissa. Lähiverkkojen yhdistäminen toisiinsa tapahtuu alueverkoilla ethernet-tekniikalla. Ennen alueverkot määritettiin usein Frame Relay- tai ATM-tekniikoilla, mutta ne ovat väistyneet uudempien 1GE- ja 10GE-ethernetien tieltä vanhana tekniikkana runkoyhteyksissä. (Wikipedia 2015a.)

Tärkeimpiä aktiivilaitteita lähiverkoissa nykyään ovat kytkimet, jotka siirtävät tietoa lähiverkon sisällä. Yleisesti lähiverkosta löytyy myös reititin, joka siirtää lähiverkon tiedon laajaverkkoon eli WAN:iin. Yleistyneiden verkkouhkien ja verkkohyökkäyksien myötä myös palomuurit ovat lisääntyneet lähiverkkojen laitteina. Tärkeimpiä tekniikoita ovat IEEE 802 -lähiverkkotekniikat Ethernet ja WLAN. (Wikipedia 2015a.)

2.2.1 Ethernet

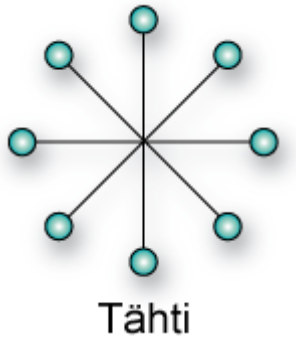
Ensimmäinen ja yleisin, laajasti hyväksytty tekniikka lähiverkossa, on pakettipohjainen lähiverkkoratkaisu, Ethernet. Sen nimi on lähtöisin yhteisestä viestiavaruudesta ja kommunikaatioon käytetystä jaetusta väylästä, maailmaneetteristä. Nykyisin nimi viittaa lähiverkkojen CSMA/CD-kilpavaraustekniikkaan perustuviin toteutustapoihin tiedon jakamisessa työasemien välillä. Kuvan 12 OSI-mallin ensimmäinen ja toinen kerros kuljettavat paketteja Ethernet-verkossa, jonka tekniikat ovat standardoitu IEEE 802.3- työryhmässä. Jotta FastEthernetin käyttöön voidaan siirtyä, vaaditaan vähintään Cat5(e)-luokan parikaapelointi. Cat5(e) siirtää dataa 100/1000 Mb/s nopeudella ja Cat6, joka on tällä hetkellä yleisin, 1000 Mb/s nopeudella. Tämän parikaapeloinnin myötä voidaan myös käyttää kaksisuuntaista full-duplex -liikennettä perinteisen half-duplex -vuorosuuntaisen liikenteen sijaan. (Wikipedia 2015b.)

Kuva 12. OSI-malli

Ethernet-lähiverkkotekniikkaa varten on olemassa standardi, IEEE 802.3. Alkuperäiseen Ethernet-määritykseen verrattuna tärkeimmät erot ovat siinä, miten paketit kehystetään siirtoa varten lähiverkossa ylemmän kerroksen protokollissa. Muutoksen myötä 802.3-standardissa esimerkiksi IP-paketteihin lisättiin kahdeksan tavua ylimääräistä tietoa LLC- ja SNAP-kehysten myötä. Yleisimmät IEEE 802.3 -standardit ovat 802.3u (100BASE-T Fast Ethernet, 100 Mb/s) ja 802.3ab (1000BASE-T Gigabit Ethernet parikaapelissa, 1 Gb/s). (Wikipedia 2014a.)

2.2.2 Verkkotopologia

Verkkotopologia eli tiekoneverkon perusrakenne ilmaisee, miten laitteet on liitetty toisiinsa. Väylä, rengas ja tähti ovat perustopologiota verkolle. Konkreettista koneiden toisiinsa liittämistä ilmaistaan fyysisellä topologialla, joka ei ota kantaa johdoissa liikkuvien pakettien tapaan liikkua. Looginen rakenne voi olla erilainen kuin fyysinen rakenne, mikä ilmenee verkossa liikkuvien pakettien tarkastelemisen avulla. (Wikipedia 2015c.)



Kuva 13. Tähtitopologia

Tähtitopologiassa (Kuva 13) kaikki tietoliikenne verkossa kulkee kytkimen kautta, johon liitetään verkon laitteet. Yhteys toisille laitteille tai verkoille kulkee keskuslaitteen eli kytkimen kautta, joka on kytketty toisiin kytkimiin tai reitittimeen. Kytkintä käytettäessä Ethernet-verkko ei ruuh-

kaudu, koska laite ohjaa paketit vain niille tarkoitettuun osoitteeseen perustuen ARP-taulun MAC-osoitteisiin. Yleisin Ethernet-verkkotopologia, joka on käytössä, on tähtitopologia. Sen etuna on esimerkiksi yhden kaapelin rikkoutumisen vaikuttamattomuus muun verkon toimintaan. Koaksiaali-, valokuitu- ja kierretty parikaapeli ovat yleisimpiä kaapeleita tähtirakenteisessa lähiverkossa. (Wikipedia 2015c.)

2.2.3 Palomuuri

Tietoverkoissa palomuurin tehtävänä on suodattaa suojatun ja avoimen verkon välinen liikenne. Sen tarkoituksena on estää avoimesta verkosta, esimerkiksi internetistä, tulevia verkkohyökkäyksiä. Palomuurilla suodatetaan saapuvaa verkkoliikennettä erilaisilla säännöillä tarvittavaa minimiä lukuun ottamatta. Myös lähtevän liikenteen suodatus on yleistynyt nykypäivinä vastuullisen verkon käytön myötä. Myös tietosuojan turvaaminen on osatekijänä lähtevän liikenteen suodatukseen. (Wikipedia 2015d.)

Tilallisen palomuurin tehtävänä on tarkastaa paketin sille saapuessa, onko sillä joku yhteyteen oleva sääntö, minkä perusteella paketti lasketaan läpi. Esimerkiksi TCP-yhteyden auetessa palomuuri vertaa protokollaa olemassa oleviin sääntöihin, mihin nojautuen data joko hyväksytään tai hylätään. Yleensä paketin protokollaan liittyvät ICMP-sanomat myös hyväksytään. Tilallisen palomuurin ongelma on, että palaavan liikenteen portteja ei voida kaikissa protokollissa tietää. Pakettisuodatus toimii OSI-mallin neljännellä kerroksella, eli kuljetuskerroksella. Nykyään useimmat työasemien palomuurit ovat yhdistelmä sovellus- ja tilallisesta palomuurista. Näin ollen ne pystyvät tarkkailemaan myös pakettien sisältöä ja sen perusteella suodattamaan laittomia komentoja sisältävää liikennettä. Toiminnallisuuden kannalta on huomattavaa, että paketin palaava liikenne on aina sallittu. (Wikipedia 2015d.)

Toimeksiantajalla on käytössä Ciscon palomuuri, joten teoria rajoittuu kyseiseen laitteeseen ja sen Best Practices -käytäntöihin. Ciscon mukaan verkossa on kolme toiminnallista tasoa, jotka on suojattava.

- Hallinnointitaso, joka hoitaa palomuurille lähetettyä liikennettä, joka koostuu sovelluksista ja protokollista, kuten SSH ja SNMP.
- Ohjaustaso, joka käsittelee verkkoinfrastruktuurin kannalta tärkeän liikenteen. Ohjaustaso koostuu verkkolaitteiden välisen liikenteen protokollista ja sovelluksista, kuten EIGRP:stä ja OSFP:stä.
- Datataso, joka ohjaa verkkoliikenteen palomuurin läpi.

Teoria ei ota kantaa laitteen konfiguroinnin tarkasteluun, poikkeuksena Best Practises Checklist liitteessä 3. (Cisco n.d.a.)

2.3 Palvelimet

Palvelinten osalta teoria rajautuu siihen, mitä palvelimille oli alkutilanteessa asennettu ja mitä uuteen ympäristöön asennetaan. Asennukset eivät sinällään ole mitään ohjelmistoja vaan palvelimen omia rooleja ja ominaisuuksia. Näitä ovat:

- Active Directory Domain Services
- Domain Name System
- Group Policy Management
- File and Storage Services
- Windows Server Update Services
- Windows Deployment Services
- Print Services.

Teoria rajataan siihen, miten Microsoft määrittää suunnittelun ja toteutuksen sekä Best Practises -mallit. Palvelinten osalta teoriassa ei myöskään oteta kantaa siihen, miten ne tulisi yksityiskohtaisesti konfiguroida, vaan tämä käy ilmi suunnittelussa, jossa perehdytään tarkemmin tarvittaviin ja suositeltuihin asetuksiin. Myös testaus ja toteutus -vaiheessa asiaa käsitellään Microsoftin Best Practises Analyzer -työkalun myötä.

2.3.1 Active Directory Domain Services

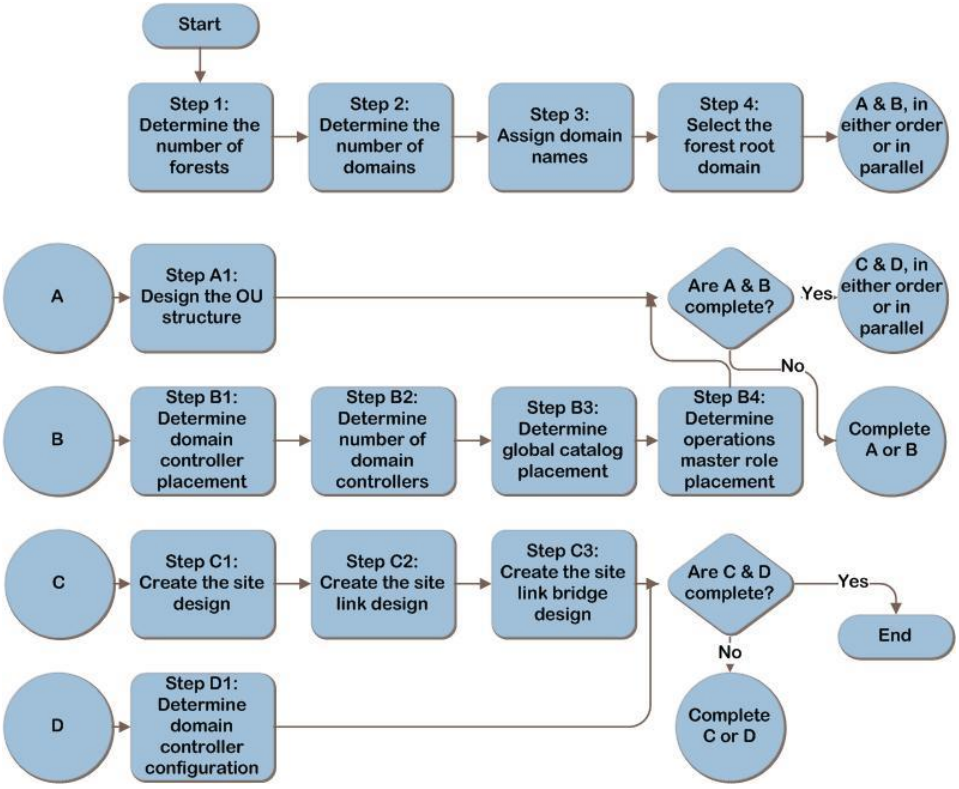
Active Directory (AD) on Microsoftin toteutus LDAP-hakemistopalvelusta. Tämä voidaan käsittää tietokantapalveluna, joka on tarkoitettu samankaltaisten objektien tallentamiseen. Lajittelu tapahtuu loogisilla ja hierarkisilla tavoilla objektien attribuuttien perusteella. (Wikipedia 2014b.)

Tietoverkoista puhuttaessa Directory Services (DS) ilmaisee tapaa, jolla tietoa tallennetaan organisoidusti tietoverkon laitteista ja käyttäjistä. Se tarkoittaa myös hallinnointitapaa, jolla pääkäyttäjät pääsevät resursseja hallinnoimaan. Hakemistopalvelulla tarkoitetaan lisäksi tiettyä abstraktia tasoa, joka hallinnoi käyttäjien pääsyä resursseihin. (Microsoft 2013.)

Active Directoryn ylimmällä tasolla, joka sisältää kaikki objektit, attribuuttimäärittelyt ja säännöt, on forest. Siinä voi olla yksi tai useampi muuttuva puu, jolla on toisiinsa nähden luottosuhteita. Jokainen puu on domain tai domain-puu ja niitä muodostuu yksi tai useampi ja ne ovat yhdistetty muuttuvaan luottohierarkiaan. (Microsoft 2013.)

Active Directory Domain Services (AD DS) kontrolloi ydinturvallisuutta Windows-verkkoympäristössä. Hakemistopalvelu vastaa käyttäjä- ja tietokonetilien todentamisesta AD DS -infrastruktuurin sisällä. Lisäksi hakemistopalvelu tarjoaa mekanismin keskitettyyn ja delegoituun hallinnointiin resurssien forestissa. (Microsoft 2013.)

Onnistuneen AD DS:n kehittämiseen ja suunnittelemiseen kuuluvat monien strategioiden määritykset sekä lukuisten päätösten tekeminen (Kuvio 1). Kriteereistä muun muassa suorituskyky, turvallisuus, hallittavuus ja skaalautuvuus on selvitettävä, jotta voidaan päästä hyvään tulokseen. (Microsoft Solution Accelerators 2011, 2.)



Kuvio 1. Kriittinen polku ja AD DS -suunnittelun prosessin kulku

Active Directory forestissa, yhdessä domainissa, on viisi operations master -roolia.

Schema Master on domainohjain, joka isännöi schema master -roolia. Se vastaa päivitysten käsittelystä Active Directory -schemaan. Tämä FSMO-rooli on forestissa ylimmän tason domainissa. (Microsoft 2014.)

Domain Naming Master on forest-tason FSMO-rooli, mikä tarkoittaa, että on vain yksi domain controller Active Directory -forestissa, jossa kyseinen rooli on. Se on vastuussa verkkotunnusten ja loogisten osioiden lisäämisestä ja poistamisesta forestissa. Tietokone, joka isännöi tätä roolia, on myös vastuussa referenssien hallinnoinnista toisiin toimialueisiin eri foresteissa, joilla on luottosuhde päätason forestin kanssa. (Microsoft 2014.)

PDC-emulaattori on domainpohjainen rooli, joka hallinnoi seuraavat asiat:

- Verkkotunnusten salasanojen vaihtamisen hallinta: PDC-emulaattori varmistaa, että salasanojen vaihto replikoidaan muihin toimialueen ohjauskoneisiin mahdollisimman pian.
- Ajan synkronointi koko domainin jäsenille: Koska PDC-emulaattorit alidomaineissa synkronoivat aikansa päätason domainin kanssa, tulee varmistaa että päätason toimialueen ohjauskone, jolla PDC-emulaattorin rooli on, synkronoi aikansa jostakin luotetusta ulkoisesta lähteestä. Näin taataan kaikille koneille forestissa oikea aika.
- Group Policy muutokset: PDC-emulaattori varmistaa, ettei synny konflikteja tapauksissa, joissa GPO on kahden tai useamman käyttäjän muokattavana samanaikaisesti.

– Domain master -selain: PDC-emulaattori tarjoaa luettelon työryhmistä ja toimialueista kun verkkoa selataan.

(Microsoft 2014.)

Infrastructure master on domain controller, joka pitää kirjaa forestissa muihin domaineihin tehdyistä muutoksista ja niiden vaikutuksesta paikallisen domainin objekteihin. Jokaisessa domainissa yhdessä forestissa on domain controller, jolla on kyseinen rooli. (Microsoft 2014.)

RID on domain-tason FSMO-rooli, joka käsittelee pyynnöt suhteellisista tunnisteista (RIDs). Aina kun käyttäjä-, ryhmä-tai tietokoneen tili on luotu domainiin, kyseiselle objektille on muodostunut suojaustunniste (SID). SID koostuu domainin SID-tunnisteesta ja uniikista RID-tunnisteesta. Nämä kaksi tunnistetietoa ovat RID-roolin tuottamia. (Microsoft 2014.)

Schema Master ja Domain Naming Master ovat näistä rooleista uniikkeja ja niitä voidaan pitää vain yhdellä DC:llä metsässä. Muut roolit ovat läsnä jokaisessa domainissa samassa forestissa. (Microsoft 2014.)

Active Directoryn suojaus käsitellään suunnitteluvaiheessa kappaleessa 5.1.1. AD DS:n asennus ja konfigurointi tapahtuu joko graafisesta käyttöliittymästä tai powershell-komentoriviltä perustuen AD DS Best Practices -menetelmiin, jotka ovat esiteltynä liitteessä 4. (Microsoft 2012.)

2.3.2 DNS

Domain Namin System (DNS) on järjestelmä, jota käytetään TCP/IP-verkkojen tietokoneiden ja verkon palveluiden nimeämiseen. Järjestelmä etsii tietokoneiden ja palveluiden käyttäjäystävälliset nimet perustuen laitteiden FQDN- ja IP-osoitteen relaatioon. DNS-tietokanta koostuu useista erilaisista resurssitietueista, joita on olemassa useanlaisia. Jokainen yksittäinen resurssitietue tunnistaa eri tietueet tietokannassa. Yleisimpiä resurssitietueita ovat:

– Start of authority
– Host
– Name server
– Mail Exchanger
– Canonical name.

(Microsoft n.d.b.)

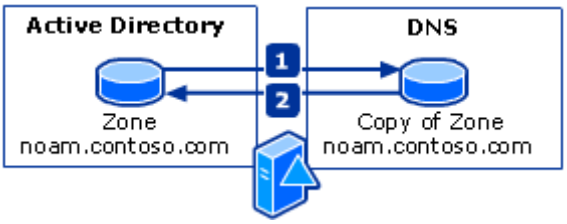
DNS-tietokanta voidaan osittaa useisiin vyöhykkeisiin. Vyöhyke sisältää resurssitietueiden omistajien nimet, jotka kuuluvat DNS-tietokannan nimiavaruuteen. Vyöhyketiedot sijaitsevat DNS-palvelimilla, jotka voidaan asettaa isännäksi yhdelle tai useammalle vyöhykkeelle. On myös mahdollista, että palvelin ei sisällä yhtään vyöhyketietoa. (Microsoft n.d.b.)

Jokainen vyöhyke on kiinni päätason verkkotunnuksessa. Vyöhyke sisältää tietoa kaikista nimistä, jotka päättyvät päätason verkkotunnukseen. DNS-palvelinta pidetään määräävänä (Start of Authority), jos se sisältää vyöhykkeen, jolta nimeä haetaan. Ensimmäinen tietue millä tahansa vyö-

hykkeellä on määräävän palvelimen tunnus. Se tunnistaa primääri DNS-palvelimen parhaan tietolähteen vyöhykkeen kyselyn ja kokonaisuutena prosessoi vyöhykkeiden päivityksen. (Microsoft n.d.b.)

Vyöhykkeellä sijaitseva nimi voidaan delegoida toiselle vyöhykkeelle, jota isännöi eri palvelin. Tarkoituksena on siirtää nimiavaruuden osa hallittavaksi toiselle osapuolelle, joka voi olla esimerkiksi toinen organisaatio, osasto tai työryhmä samassa yrityksessä. Vyöhykkeen delegointia edustaa Name Server -tietue, jolla määritetään toinen määräävä DNS-palvelin kyseiselle vyöhykkeelle. Yleisimpiä syitä delegointiin ovat hallinnoinnin siirto ja kuorman jakaminen useamman palvelimen välillä suorituskyvyn ja virheensiedon parantamiseksi.
Nimiavaruuden samaa osaa edustavia vyöhykkeitä voi olla useita. Ensisijainen on vyöhyke, johon kuuluviin tietoihin kaikki muutokset tehdään. Toissijainen on pelkästään ensisijaisen kopio, jota vain luetaan. Kaikki muutokset, jotka tehdään ensisijaiseen, replikoituvat myös toissijaiseen.
Replikointiprosessia DNS-palvelinten välillä kutsutaan vyöhykkeen siirroksi, joka saavutetaan kopioimalla vyöhykkeen tiedot palvelimesta toiseen. (Microsoft n.d.b.)

DNS-palvelu on suunniteltu myös integroitavaksi Active Directoryn kanssa, jolloin AD:ta käytetään tietojen ja replikoinnin lähteenä (Kuva 14). DNS-replikointi suoritetaan Active Directoryn toimesta, jolloin erillistä replikointitopologiaa ei tarvita DNS-palvelinten välillä. Se on myös turvallinen ja tietueiden päivitys vyöhykkeisiin ei ole riippuvainen määräävästä DNS-palvelimesta, vaan tietueiden ja vyöhykkeiden muutos voidaan tehdä mille tahansa toimialueen ohjaimelle. (Microsoft n.d.b.)



Kuva 14. Active Directory -integroitu vyöhyke

Kun replikointi tapahtuu Active Directoryn kautta, vyöhyke kopioidaan muille toimialueen ohjaimille samassa domainissa. DNS-palvelin voi myös lähettää kopion vyöhykkeestä sille toissijaiselle DNS-palvelimelle, joka sitä on pyytänyt, perustuen standardiin vyöhykkeen siirtoon. Vyöhykkeen siirto voi olla täysi tai osittainen. (Microsoft n.d.b.)

Active Directory -integroidut alueet tallennetaan toimialueen laajuisiin hakemistoihin, joihin sisältyvät seuraavat tiedot:
- reverse lookup zone
- forward lookup zone
- root hints.

(Microsoft n.d.b.)

Yleensä DNS-kyselyissä käytetään Forward Lookup -määritystä verkkotunnuksen relaatioon IP-osoitteeseen. Tällöin kysely lähetetään nimenä,

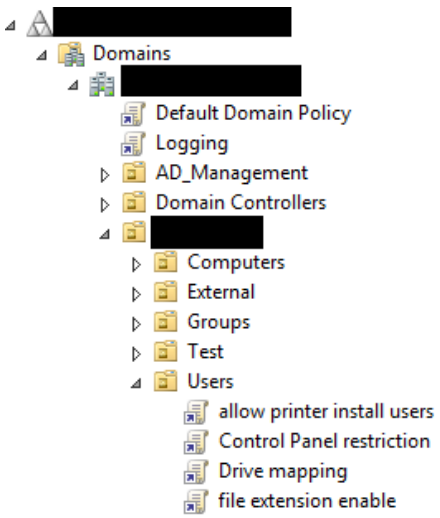
jolloin DNS etsii kysytylle nimelle IP:n. Reverse Lookup toimii päinvastoin IP-osoitteen relaationa verkkotunnukseen. Käänteisen vyöhykkeen tietokanta sijaitsee päätason toimialueessa (arpa) ja tietueiden tyyppinä on pointer (PTR). (Wikipedia 2015e.)

DNS-roolin asennus ja konfigurointi tapahtuu joko graafisesta käyttöliittymästä tai powershell-komentoriviltä perustuen best practices -käytäntöihin (Liite 5).

2.3.3 Group Policy Management

Group Policy on infrastruktuuri, jonka avulla voidaan toteuttaa erityisiä kokoonpanoja käyttäjille ja tietokoneille. Ryhmäkäytäntöasetukset sisältyvät ryhmäkäytäntöobjekteihin, jotka liittyvät Active Directory -hakemistopalvelussa site-, domain- ja organisaatioyksikkö-containereihin (Kuva 15). Ryhmäkäytäntöobjektien asetukset arvioidaan sen jälkeen vaikuttavissa kohteissa käyttäen AD:n hierarkista luonnetta. (Microsoft 2011.)

Jokaisessa ryhmäkäytännössä, joka voidaan käyttäjä- tai konekohtaisesti asettaa, on olemassa kaksi eri asetusta, Policies ja Preferences. Policies avulla voidaan määrittää käytäntöasetukset, joita group policy valvoo. Preferences avulla voidaan määrittää melkeinpä mikä tahansa rekisteriarvo, esimerkiksi poistaa käytöstä jokin kansio käyttäjän tietokoneelta. (Microsoft 2011.)



Kuva 15. GPO Management -konsoli

Ryhmäkäytäntöobjektit käsitellään seuraavassa järjestyksessä:

- Paikallinen: Sisältää kaikki asetukset lokaalisti.
- Site: Mikä tahansa Active Directory Site, jolla tietokone on.
- Domain: Mikä tahansa ryhmäkäytäntö, joka on Windows-domainissa.
- OU: Ryhmäkäytännöt, jotka on asetettu kyseiseen OU:iin, jossa käyttäjä- tai tietokonetili sijaitsee.

Mikäli edellä mainituilla tasoilla on useampi ryhmäkäytäntö tasoa kohden, ne prosessoidaan siinä järjestyksessä, kuin ne ovat ylläpidon toimesta

määritelty. Ryhmäkäytännöt myös periytyvät hierarkiassa ylimmältä tasolta alaspäin, mikäli periytymistä ei katkaista. (Microsoft 2011.)

2.3.4 File and Storage Services

Tiedostopalvelin on verkkoon liitetty tietokone, jonka tarkoituksena on toimia varastona jaetulle materiaalille verkossa. Tiedostopalvelimen ei ole tarkoitus suorittaa laskennallisia toimia, vaan varastoida ja hakea tietoa kun itse suorite tapahtuu työasemilla. (Wikipedia 2015f.)

Windowsissa on kaksi käyttöoikeutta tiedostoille ja kansioille, share- ja NTFS-oikeudet. NTFS-oikeuksia kutsutaan myös suojausoikeuksiksi (Kuva 16). Kansioiden käyttöoikeudet tehdään yleensä käyttämällä yhdistelmää molemmista, jolloin tulee noteerata, että kaikkein rajoittavin tekijä on voimassaoleva. Käyttäjätunnukset ja ryhmät ovat alfanumeerisia merkkijonoja nimeltään SID, johon Share- ja NTFS-oikeudet ovat sidottuja. Share-oikeudet tarkastetaan LSASS:n toimesta, kun resurssiin hakeudutaan verkon yli. NTFS-oikeudet ovat voimassa vain paikallisesti tietokoneella. (Gibb 2011.)

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Administrators (PANNU\Adm...	Full control	None	This folder only
Allow	Administrators (PANNU\Adm...	Full control	D:\	This folder, subfolders and files
Allow	SYSTEM	Full control	D:\	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	D:\	Subfolders and files only
Allow	Users (PANNU\Users)	Read & execute	D:\	This folder, subfolders and files
Allow	Users (PANNU\Users)	Special	D:\	This folder and subfolders

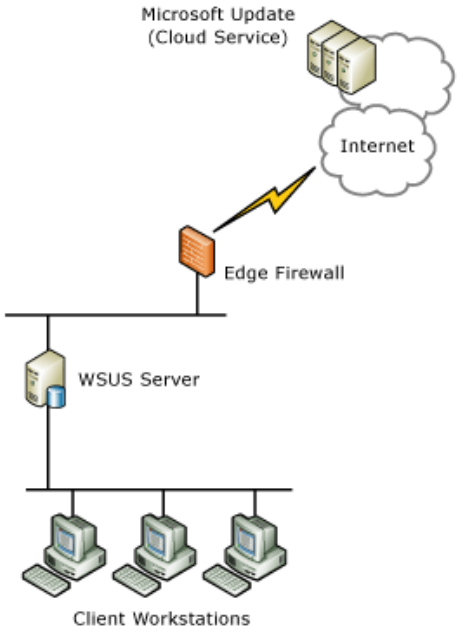
Kuva 16. Esimerkki NTFS-oikeuksista

Kun oikeudet asetetaan, LSASS kontrolloi resurssiin pääsyä. Kirjauduttaessa työasemalle, käyttäjä saa käyttöoikeusattribuutin omaan SID:iin, jota LSASS vertaa resurssin käyttöoikeuslistalta löytyvien SID:ien kanssa ja näin määrittää pääsyn tai kiellon resurssiin. (Gibb 2011.)

File Services -roolin asennus ja konfigurointi tapahtuu joko graafisesta käyttöliittymästä tai powershell-komentoriviltä perustuen best practices -käytäntöihin (Liite 6). (Microsoft 2010a.)

2.3.5 Windows Server Update Services

Windows Server Update Service (WSUS) avulla voidaan verkossa jakaa Microsoftin tuotteiden päivityksiä. Sillä voidaan hallita jokaisen päivityksen jakelua keskitetysti palvelimelta sekä seurata päivitysten edistymistä. Roolin avulla päivitykset voidaan jakaa niin työasemille kuin palvelimille. Päivitysten lähteenä toimii upstream-palvelin. joka on yhteydessä Microsoftin päivitystietokantaan (Kuva 17). Tällaisia palvelimia voi olla yksi tai useampi riippuen ympäristöstä. (Microsoft 2014a.)



Kuva 17. WSUS

Päivitysten hallinta on prosessi, joka kontrolloi ohjelmistopäivitysten käyttöönottoa tuotantoympäristöön. Sen avulla voidaan tehostaa toimintaa, hallita haavoittuvuuksia sekä ylläpitää ympäristön vakautta. Mikäli käyttöjärjestelmiä ja sovelluksia ei pidettäisi ajan tasalla, voi se johtaa useisiin tietoturva-aukkoihin. Tämä lisää liiketoiminnassa uhkaa tulojen ja tietojen menetykseen. Ydinskenaariot, joissa WSUS tuo lisäarvoa, ovat keskitetty päivitysten hallinta ja päivitysten automatisointi. (Microsoft 2014a.)

Microsoft luokittelee päivityksensä tärkeäksi, suositelluksi tai valinnaiseksi:

- Tärkeät päivitykset tarjoavat huomattavia etuja, kuten parannetun tietoturvan, yksityisyyden ja luotettavuuden.
- Suositellut päivitykset ratkovat ei-kriittisiä ongelmia tai auttavat käyttöjärjestelmän suorituskyvyssä. Vaikka kyseiset päivitykset eivät varsinaisesti ratkaise fundamentaalisia ongelmia tietokoneella, voivat ne tarjota huomattavia parannuksia funktionaalisuuteen.
- Valinnaiset päivitykset ovat yleensä uusia ohjelmia ja ajureita sekä päivityksiä jo olemassa oleviin ohjelmiin.

Päivityksien tyypeistä riippuen ne voivat tietoturvapäivityksiä, kriittisiä päivityksiä tai Service Pack -paketteja. (Regan 2013.)

Windows Server Update Services -roolin asennus ja konfigurointi tapahtuu joko graafisesta käyttöliittymästä tai powershell-komentoriviltä perustuen best practices -käytäntöihin (Liite 7). (Microsoft 2011a.)

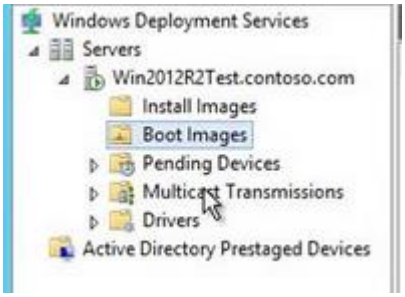
2.3.6 Windows Deployment Services

Windows Deployment Services (WDS) on ohjelmistoalusta ja tekniikka, jonka avulla voidaan tietokone asentaa verkosta, eikä varsinaista fyysistä asennusmediaa tarvita (Kuva 18). WDS tallentaa asennustiedostot ja sen avulla voidaan hallita niin levykuvia kuin käynnistystiedostoja.

Levykuva on periaatteessa jonkin hetken tilanne tietokoneen kiintolevyllä, josta on otettu kopio kyseisellä ajan hetkellä. Sitä kutsutaan myös asennuslevykuvaksi ja sitä yleensä käytetäänkin käyttöjärjestelmien asentamiseen. Levykuva sisältää seuraavat tiedot:

– Kaikki käyttöjärjestelmän tiedot tietokoneella
– Kaikki päivitykset ja asemat jotka on asennettu
– Kaikki sovellukset, mitkä on asennettu
– Kaikki tehdyt kokoonpanomuutokset.

(Regan 2013.)

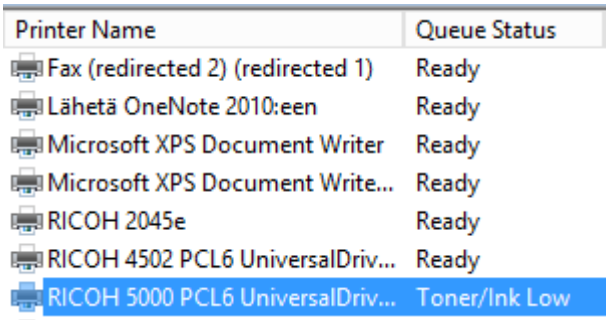


Kuva 18. WDS

Jotta tietokoneet voivat kommunikoida WDS-palvelimen kanssa, tulee niissä olla Preboot Execution Environment (PXE) -tuki. PXE on tekniikka, joka käynnistää tietokoneen käyttäen verkkokorttia ilman minkäänlaista tietovarastoa eli kiintolevyä tai käyttöjärjestelmää. Toiminto määritetään tietokoneen BIOS-asetuksista siten, että se on ylimpänä käynnistyshierarkiassa. (Regan 2013.)

2.3.7 Print Services

Tulostuksen hallinnan avulla voidaan selvittää tulostimien tila verkossa (Kuva 19). Sen avulla voidaan myös asentaa tulostimia ryhmäkohtaisesti. Roolin avulla saadaan myös paljon tietoa tulostimista, joissa on http-pohjainen hallinta. (Microsoft 2014b.)



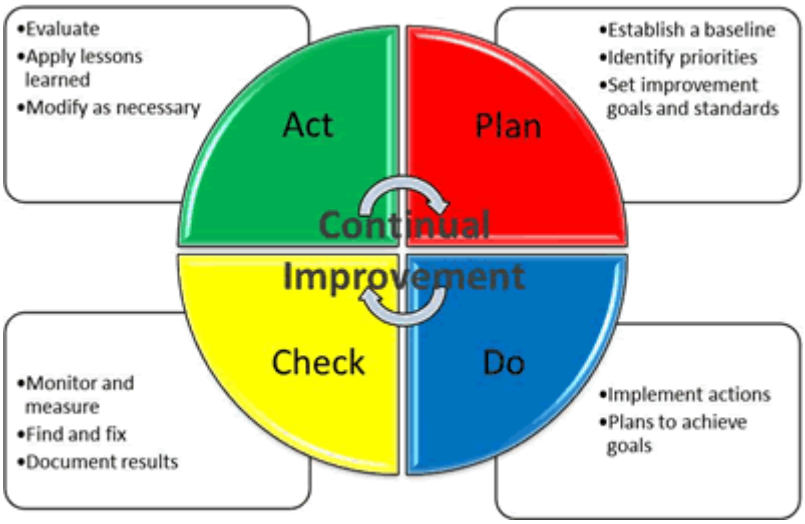
Kuva 19. Print Management

Windows Server 2012 myötä Microsoft esitteli tulostukseen uuden versio 4 -ajurin, jonka myötä tulostinajurien asennus käyttäjien työasemille tapahtuu Windows-päivitysten myötä joko lokaalisti tai WSUS:ia apuna käyttäen.

Suurimmat hyödyt ovat siinä, että tulostimen jakaminen ei vaadi laitekohtaista ajuria vallitsevassa arkkitehtuurissa ja yksi ajuri voi tukea yhtä tai useampaa laitetta. (Microsoft 2014b.)

2.4 ISO 17799:2005 / ISO27002:2005

ISO/IEC 27000 -sarja käsittää Kansainvälisen standardisoimisjärjestön (ISO) ja Kansainvälisen sähkötekniikan toimikunnan (IEC) tietoturvallisuuden standardeja. Sarja tarjoaa parhaiden käytäntöjen suosituksia tietoturva- sekä riskinhallintaan ja kontrollointiin tietoturvan hallintajärjestelmän puitteissa (ISMS). Sarjan soveltamisala on tarkoituksellisesti laaja ja se kattaa muutakin kuin kysymyksiä yksityisyydestä, luottamuksellisuudesta ja tietotekniikan tai tekniikan turvallisuudesta. Standardit soveltuvat kaiken kokoisille yrityksille, ja ISO/IEC suosittelee kaikkia organisaatioita arvioimaan omat tietoturvariskinsä, joihin pohjautuen toteuttaa omat tarpeensa asian suhteen. Koska tietoturvan luonne on dynaaminen, asioita lähestytään plan-do-check-act –periaatteella (Kuva 20), jolloin voidaan paremmin käsitellä uhkia, heikkouksia ja vaikutuksia tietoturvaan. (Wikipedia 2015g.)



Kuva 20. plan-do-check-act

Työssä käytettiin ISO/IEC 27002:2005 standardia, jonka pohjalta muodostettiin toimeksiantajalle tietoturvasuunnitelma. Tietoturvasuunnitelmaa tehtäessä ISO/IEC 27002:2013 ei ollut vielä julkaistuna, joten vanhempi versio otettiin käyttöön.

Standardi määrittelee tietoturvaa koskevia ohjeita ja yleisiä periaatteita liittyen tietoturvan käynnistämiseen, käyttöönottoon, ylläpitoon ja parantamiseen. Se tarjoaa opastusta yleisellä tasolla hyväksytyistä tietoturvahallinnan tavoitteista sekä sen käyttöönotolla tunnistetaan riskien arvioinnin vaatimukset. Standardin pohjalta luotava suunnitelma toimii käytännön ohjeistuksena, jonka pohjalta voidaan kehittää turvallisuusjohtamisen käytäntöjä sekä lisätä luottamusta liiketoiminnassa organisaatioiden välillä. (ISO/IEC 27002:2005, viii-xi.)

Standardi jakautuu seuraaviin kappaleisiin, joista tietoturvasuunnitelma muodostuu:

- Risk assessment and treatment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance.

(ISO/IEC 27002:2005, iii-vi.)

2.5 TAL-suositukset

Taloushallintoliiton mukaan tilitoimistosta tulisi löytyä tietojärjestelmien sekä käyttäjien ja asiakkaiden oikeuksien dokumentointi resursseihin. Lisäksi liitto tarjoaa itsearviointilomakkeen tietoturvallisuuden kartoittamisesta. Kokonaisuudessaan dokumentit ovat:

- Tilitoimiston järjestelmädokumentaatio
- Ohjelmistoluettelo
- Laitteistoluettelo
- Käyttäjäluettelo
- Tilitoimistohenkilön käyttäjäkohtaiset oikeudet
- Asiakkaan henkilöstön käyttäjäkohtaiset oikeudet
- Tietoturvan kartoitus tilitoimistossa

(Suomen Taloushallintoliitto, 2012.)

Kyseisiä dokumentteja tarkastellessa voidaan huomata ISO 27002:2005-standardiin perustuvan tietoturvasuunnitelman kattavan kaikki osa-alueet ja näin ollen TAL-suositusten varsinaista käsittelyä ei tarvita. Dokumentit kuitenkin otettiin huomioon, mikäli auktorisoinnin kannalta ilmenee tarve niiden täyttämiselle.

3 IT-YMPÄRISTÖN KARTOITUS

Ympäristön kartoitus tehtiin vierailemalla yrityksen tiloissa kolmen päivän ajan. Tänä aikana kerättiin tietoa kaikista projektin piiriin kuuluneista laitteista ja järjestelmistä sekä sovelluksista. Lisäksi hyödynnettiin toimeksiantajan omaa selvitystä ympäristön alkutilanteesta.

3.1 Palvelimet

Kartoitushetkellä yrityksellä oli käytössään kaksi Hewlett-Packard Proliant ML350 G5 -palvelinta, SRV1 ja SRV2. Molemmat olivat laitteistoteknisesti samanlaiset, tärkeimmiltä ominaisuuksilta seuraavat:

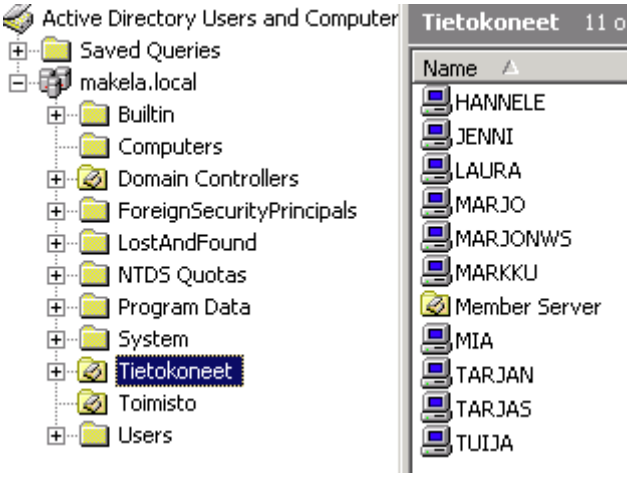
- Prosessori: Intel Xeon E5420
- RAM: 4GB
- 5 kiintolevyä, joista kaksi oli asetettu raid 1 -tilaan ja kolme raid 5 -tilaan. Näin ollen palvelimilla oli kaksi loogista kiintolevyä.
- DVD-asema
- Gigabit ethernet
- Kaksi virtalähdettä

Lisäksi kumpikin palvelin käytti samaa UPS-varavirtalähdettä.

Erona palvelimilla oli se, että SRV1:llä oli nauhavarmistin ja sillä oli voimassa oleva huoltosopimus. Molemmissa palvelimissa oli käyttöjärjestelmänä Windows Server 2003 R2. Palvelimista ei löytynyt ajantasaista dokumentaatiota, poikkeuksena huoltosopimus.

3.1.1 Active Directory

Tarkasteltaessa AD:ta voitiin todeta SRV1:n olevan domainin ja forestin ylin palvelin, jolla kaikki FSMO roolit sijaitsivat. SRV1:n ja SRV2:n välillä oli replikointi AD:n suhteen.
AD:n rakenne oli kutakuinkin samanlainen, mitä se uuden asennuksen yhteydessä aina on (Kuva 21). Toimialueen päätasolle oli tehty kaksi OU:ta, joihin oli epäsäännöllisesti sijoitettuna käyttäjätunnuksia ja työasematilejä.



Kuva 21. Vanha AD

Group Policy Management -työkalua ei ollut asennettu eikä AD:sta löytynyt yhtään GPO:ta. Hallinnointiin käytettiin Administrator-tunnusta. AD:sta ei ollut olemassa dokumentaatiota.

3.1.2 DNS

SRV1 oli Start of Authority ja näin ollen metsän ylin nimipalvelin. SRV2 toimi Name Serverinä. DNS oli Active Directory -integroitu ja scavenging-aika oli seitsemän vuorokautta. DNS-palveluun ei ollut luotu Reverse Lookup Zonea. Palvelusta ei löytynyt dokumentointia.

3.1.3 Print Services

Tulostuspalvelimena toimi SRV1. Palvelimelta löytyi monia ajureita, osa sellaisia, joiden tulostimia yrityksellä ei enää ollut. Tulostuksen spoolaus oli asetettu tapahtumaan palvelimella. Tulostuspalvelusta ei ollut dokumentointia, eikä tulostimien tilaa oltu aktiivisesti seurattu.
Yrityksen tulostimet:

- Ricoh 2045e, IP: 192.168.1.8
- Ricoh MP C4502, IP: 192.168.1.9
- Ricoh MP C5000, IP: 192.168.1.19.

3.1.4 File and Storage Services

Molemmilla palvelimilla oli jaettuja hakemistoja, jotka eivät replikoituneet palvelinten kesken. Kansioihin täydet oikeudet olivat Makela Users, Everyone, Domain Users ja Administrators-ryhmillä. Koska vain SRV1:llä oli nauhavarmistin, SRV2:n tietojen varmistus oli ratkaistu siten, että SRV2:lle oli tehty skripti, joka kopioi jaetut resurssit SRV1:lle yöaikaan ennen nauhavarmistusajoa. Palvelusta ei ollut dokumentointia.

3.2 Työasemat

Yrityksellä oli käytössä HP:n työasemia. Työasemista viisi oli uusittu hiljattain ja loput seitsemän olivat vanhempia. Käyttöjärjestelmänä oli Windows XP SP3. Työasemiin oli asennettu ohjelmia tarpeen mukaan, joten varsinaista vakioitua mallia ei ollut. Mikäli kuitenkin halutaan jonkin asteisesta yhteisestä kokonaisuudesta puhua, seuraava listaus oli kaikissa sama:

- Office 2010
- PDF Creator
- Cute PDF
- F-Secure
- Unes
- Google Chrome
- Mozilla Firefox
- Adobe Reader
- Microsoft Silverlight
- Java
- Citrix reciever
- Adobe Flash
- Cisco Webex
- Microsoft Netframework 1.1-4.0

– WinSCP.

Käyttäjillä oli paikallisen järjestelmänvalvojan oikeudet työasemiin. Työasemien kokoonpanoa, niin laitteistollisesti kuin ohjelmistollisesti, ei oltu dokumentoitu.

Työasemien tärkeimmät tekniset tiedot:
– 3GHz prosessori, vanhemmissa 2,4GHz
– 4GB RAM, vanhemmissa 2GB
– 500GB kiintolevy, vanhemmissa 250GB
– DVD-asema
– Gigabit ethernet.

3.3 Sähköpostijärjestelmät

Yrityksellä ei ollut omaa sähköpostipalvelinta. Sähköpostia ylläpiti paikallinen operaattori AinaCom Oy, jolta oli palveluna ostettu exchange-palvelut. Mail for Exchange ei ollut käytössä. Palvelukuvausta ja palvelusopimusta säilytettiin kassakaapissa.

3.4 Lähiverkko

Yrityksen tiloissa oli Cat5(e)-verkko. Verkkolaitteina olivat seuraavat:
– Cisco reititin (Internet-palveluntarjoajan hallinnassa)
– Cisco PIX 501 -palomuuri, konfiguraatio liitteessä 8
– HP Procurve -kytkin
– Access Point (WLAN)
– Avaya-puhelunohjausjärjestelmä.

Yrityksen sisäverkkona oli C-luokan IPv4-verkko 192.168.1.0/24, verkossa ei ollut VLAN-alueita. Palomuuri toimi myös reitittimenä, jolla oli otettu käyttöön NAT ja DHCP. DHCP:n lease time oli 2 vuorokautta. DHCP jakoi osoitteet 192.168.1.10-192.168.1.129. Yrityksellä oli oma julkinen IP-avaruus xxx.xxx.xxx.xxx/29 sekä tilitoimistomakela.fi verkkotunnus. IPv6 ei ollut käytössä ja verkosta ei löytynyt dokumentaatiota.

3.5 Tietoturva

Virustorjuntaohjelmistona työasemilla oli F-Secure ja palvelimissa McAfee. Lisäksi työasemat ja palvelimet käyttivät Windowsin omaa palomuuria. Yrityksen tiloissa oli lukittava, paloturvallinen holvi, jossa säilytettiin arkistoitua materiaalia. Holvissa oli myös kassakaappi, jossa pidettiin sopimukset ja varmistusnauhat. Työhuoneissa säilytettävä materiaali oli kansioissa ja ne olivat merkittyinä asiakasnumeroin. Yrityksellä ei ollut tietoturvasuunnitelmaa eikä Disaster Recovery Plania.

3.6 Varmistukset

SRV1–palvelin oli kokonaan nauhavarmistettu. Nauha vaihdettiin vuorokauden välein ja nauhat säilytettiin holvissa olevassa kassakaapissa. Työasemilta tiedostot tallennettiin SRV2:een. SRV2:lta tiedostojen tuli kopioitua SRV1:lle skriptin avulla ja näin ollen tallentua nauhalle varmistuksen yhteydessä. Sähköinen kirjanpitoaineisto tallennettiin DVD-levyille kerran vuodessa. DVD-levyt säilytettiin holvissa.

3.7 Etäyhteydet

Yrityksellä olisi ollut mahdollista käyttää yhteyksiä etätyöskentelyyn. Vaihtoehtoina olivat VPN-yhteys tai suora RDP-yhteys palvelimiin. Toimeksiantajan mukaan yrityksellä ei kuitenkaan ole ollut tarvetta avata yhteyksiä suoraan verkkoon yrityksen tilojen ulkopuolelta.

Yrityksellä oli käytössä Aditron tarjoamana SaaS-palvelu taloushallinnon ohjelmiin, jota oli mahdollista käyttää etätyöskentelyyn Citrix-ohjelman avulla. Tämä oli käytössä kaikilla käyttäjillä myös etämahdollisuutena.

3.8 Palvelut

Yrityksellä oli kolme varsinaista kolmannen osapuolen palvelua käytössä. Aditro tarjoaa pilvipalveluita SaaS-menetelmällä, jossa toimeksiantajan taloushallinnon ohjelmistot sijaitsivat. Toinen palveluntarjoaja oli AinaCom, jolta yrityksellä oli käytössä internet-palvelut ja sähköpostipalvelut. Kolmas palveluntarjoaja oli viaInnox, jolta yrityksellä oli käytössä tehtävien ja työajan seuranta -sovellukset.

4 IT-YMPÄRISTÖN ANALYSOINTI

Ympäristön analyysi suoritettiin kartoituksen pohjalta kerätyistä tiedoista. Tuloksia verrattiin kappaleessa kaksi esiteltyihin teorioihin ja parhaisiin käytäntöihin. Lisäksi hyödynnettiin opinnäytetyön tekijän työkokemukseen pohjautunutta tietoa ja taitoa.

4.1 Palvelimet

Palvelimet ovat vuodelta 2008 ja niiden elinkaari on loppumaisillaan. Teholisesti palvelimet vielä suoriutuvat siitä kuormasta, mikä niillä on käsiteltävänä. Tarkasteltaessa muistin ja suorittimien käyttöä palvelimet eivät normaalissa kuormituksessa joudu tekemään paljoakaan työtä. Palvelimilla on käytössä vain yksi verkkokortti, mutta sen kapasiteetti riittää kaiken tarvittavan tiedon siirtämiseen. Palvelimissa on lisäksi käyttöjärjestelmä, jonka tuen Microsoft lopettaa kesäkuussa 2015. Näin ollen päivityksen tarve on suuri.

Toimeksiantajan mukaan SRV1:n huoltosopimus on uusittu ja se kattaa seuraavat kaksi vuotta. SRV2:n huoltosopimusta ei ole uusittu ja toimeksi-

antajan toive onkin ollut luopua kyseisestä palvelimesta. Tämä on siinä mielessä hyväksyttävää, jos tilalle hankitaan uusi palvelin. Näin ollen kriittiset palvelut pysyvät edelleen kahdennettuina.

4.1.1 Active Directory

Tarkasteltaessa OU-rakennetta voidaan huomata, että sitä ei ole toteutettu Microsoftin hyvien menetelmien mukaisesti. Käyttäjätilejä on ripoteltuna eri hakemistojen alle ilman mitään logiikkaa. Lisäksi käyttäjät kuuluvat ryhmään, joka on osa Domain Admin -ryhmää. Näin ollen kaikilla käyttäjillä on järjestämänvalvojan oikeudet koko toimialueeseen. Tämä johtaa yleisellä tasolla koko toimialueen tietoturvariskiin ja siihen että tietämätön käyttäjä voi tehdä admin-tasolla kaiken.

Työasematilit ovat myös monessa eri OU:ssa, joka niin ikään on huono toteutus. Tilien tulisi sijaita kootusti yhden OU:n alla, jotta niitä voidaan keskitetysti hallita. Vanhat jo käytöstä poistuneet työasemat omaavat tilin AD:ssa ja niitä ei ole poistettu työaseman poistumisen myötä. Sama tilanne on vanhojen käyttäjätunnusten kohdalla, jotka ovat myös aktiivisina. Lisäksi käytössä on default-containereita, joihon käyttäjiä ja työasemia on laitettu. Näin ei tulisi toimia, vaan kaikille työasemille ja käyttäjille olisi tullut tehdä omat paikat erikseen.

Tarkemmin tarkasteltuna voidaan huomata AD:n sisältävän todella vanhaa metadataa. Tämä ilmeni siten, että DNS antoi vuoden 2004 tietoja nimipalveluun, kun sen tietokanta replikoitiin. Tämä johtaa siihen, että uuden palvelimen migrointi saattaa aiheuttaa suurempiakin ongelmia. Toimeksiantajan osalta tilanne tiedostettiin ja näytettiin vihreää valoa tarpeelle tehdä kokonaan uusi toimialue. Hyväksi asiaksi voidaan todeta AD-palvelun oleva kahdennettuna SRV1 ja SRV2 välillä.

4.1.2 DNS

Hyvänä asiana voidaan pitää DNS:n vyöhykkeiden olevan AD-integroituja ja päivittyvän dynaamisesti vain luotettavista lähteistä. Vyöhykkeiden replikointi on sallittu ainoastaan sisäverkon palvelinten välillä ja palvelinten palomuureilta on sallittu ainoastaan tarvittava liikenne DNS-palvelulle. Palvelu käyttää myös ulkoisiin nimikyselyihin internet-palveluntarjoajan DNS-palvelimia.

Palvelinten ja DNS-palvelua käyttävien laitteiden välille ei ole määritelty IPSec-liikennettä. Tämä voi johtaa mahdolliseen tietoturvaukkoon, jolloin nimipalvelun tietoa voidaan manipuloida. Verkon monitorointi ei myöskään ole käytössä. DNS:n juuripalvelimia ei ole hallinnoitu, jolloin nimipalvelusta löytyy palvelimia, jotka eivät vastaa kyselyihin.

4.1.3 Print Services

SRV1-palvelimella on tulostuspalvelu, jonne kaikki toimipisteen tulostimet on asennettu. Palvelimella on myös tulostimien ajurit, jotka voidaan

ladata työasemille tulostimen asennuksen yhteydessä. Spoolaus tapahtuu palvelimella, mikä nostaa palvelimen kuormaa, ei kuitenkaan merkittävästi. Voidaan todeta tulostuksen olevan kunnossa.

4.1.4 File and Storage Services

Tarkasteltaessa hakemistorakennetta voidaan todeta sen olevan ison muutoksen edessä. Kansiorakenne ei vastaa mitään standardia tai hyvää tapaa toteuttaa hakemistopalvelu. Rakenne on varsin raskas, koska kansioita ja alikansiota on paljon. Tämä aiheuttaa turhaa kiintolevyjen käyttöä, jolloin luku- ja kirjoitusaika huononee. Jokaiseen kansioon on kaikilla rajaton pääsy. Huolestuttavaa on se, että rakenteeseen ja tiedostoihin pääsevät käsiksi myös ne, jotka eivät kuulu toimialueeseen. On riittävää, että on samassa verkossa. Kansioita ja tiedostoja ei siis varsinaisesti ole luvitettu AD-ryhmillä millään muotoa.

4.2 Työasemat

Työasemien tarkastelu jaoteltiin kahteen ryhmään, uusiin ja vanhoihin työasemiin. Näin pystyttiin määrittelemään tarve mahdollisten uusien hankintojen suhteen.

Uudet työasemat on uusittu vuoden 2012 aikana ja vastaavat laitteistoltaan yrityksen tarpeita. Vanhat työasemat ovat vuodelta 2009 ja alkavat olemaan jo hiukan tehottomia. Vanhempien työasemien uusiminen olisi syytä toteuttaa projektin yhteydessä. Käyttöjärjestelmänä kaikissa työasemissa on Microsoft Windows XP SP3. Microsoft lopetti tuen kyseiselle käyttöjärjestelmälle huhtikuussa 2014, joten päivittäminen oli todella ajankohtainen.

Ohjelmisto kaikissa työasemissa on varsin uutta ja niiden uusimiseen ei ole tarvetta. Kuitenkin kaikki ajurit sekä ilmaisohjelmat työn tukemiseen tulisi päivittää uusimpiin. Näin on myös toimittu, mutta se on tehty työasemakohtaisesti käyttäjien toimesta.

Työasemiin ei ole kohdistunut mitään keskitettyä hallintaa ja näin ollen virheensieto on alhaisempaa. Lisäksi mahdollisten vikatilanteiden ja epäsopivuuksien hallinta on heikompaa ja analysointi vaikeampaa.

4.3 Sähköpostijärjestelmät

Sähköpostijärjestelmät ovat paikallisen operaattorin AinaComin hallinnassa. Opinnäytetyö ei ota kantaa kolmansien osapuolten järjestelmiin. Toimeksiantajan mukaan palvelu on toiminut moitteetta.

4.4 Lähiverkko

Yrityksen palomuuri on vanha ja se tarvitsee uusia. Cisco on lopettanut laitteelle tuen heinäkuussa 2013. Konfiguraatiota tarkasteltaessa voidaan

ottaa esille snmp-communityn olevan public, joka ei noudata parhaita menetelmiä. Lisäksi käytössä on mahdollisuus telnet-yhteyteen sisäverkosta, jota käytettäessä liikenne on salaamatonta. Ongelma voi muodostua myös DHCP:n ja DNS:n erilaisista vanhentumisajoista. DHCP:n IP-osoitteiden vanhenemisajan ollessa pienempi kuin DNS:n, on mahdollista, että yksi nimi voi saada kaksi eri IP-osoitetta. Muilta osin asetukset ovat kunnossa toimivuuden ja tietoturvan osalta.

Fyysisen verkon ollessa Cat5e luokiteltu, on sen nopeus riittävä yrityksen tarpeisiin. Verkon teoreettinen maksimisiirtokapasiteetti on 125 megatavua sekunnissa, jolloin jokaiselle verkon laitteelle samanaikaisessa käytössä jää teoreettiseksi nopeudeksi noin 7,3 megatavua sekunnissa.

Yrityksen kytkin on ei-hallittava. WLAN ei ole käyttäjien käytössä, vaan sillä on toteutettu IP-kameran kuvan tiedonsiirto. Yhteys on WPA2-PSK (AES) salattu, joka on turvallisin ratkaisu.

4.5 Tietoturva

Laitteistokohtaisesti ajateltuna tietoturva on osittain kunnossa. Työasemilla ja palvelimilla on uusimmat versiot virustorjunnasta ja konekohtaiset palomuurit käytössä. Haavoittuvuutena voidaan pitää käyttäjien järjestelmänvalvojan oikeuksia.

Suurin puute kuitenkin on tietoturvasuunnitelman puuttuminen, jolloin ei ole olemassa minkäänlaisia menettelyohjeita tai -tapoja tietoturvapoikkeamien sattuessa. Henkilökuntaa ei näin ollen ole myöskään koulutettu toimimaan poikkeaminen varalta.

Yrityksen paperilla, nauhavarmenteilla ja DVD-levyillä olevat tiedot ovat turvassa holvissa. Holvi on lukittu ja se on paloturvallinen. Holvissa on kassakaappi, jossa säilytetään tärkein aineisto. Näiltä osin tietoturvan voidaan todeta olevan kunnossa.

4.6 Varmistukset

Hakemistopalvelun rakenne sijaitsee SRV2-palvelimella, josta on toteutettu ajastetulla toiminnolla koko kansiorakenteen kopiointi SRV1-palvelimelle, jotta tiedot saataisiin varmistettua nauhavarmistimella. Tämä toiminto ei kuitenkaan toimeksiantajan mukaan tällä hetkellä toimi ja näin ollen kaikki tieto on SRV2:n kiintolevyllä varmistamatta. Kartoituksen aikana tätä tapahtumaa seurattiin ja voitiin todeta toimimattomuus.

Kolmansien osapuolten tuottamissa palveluissa varmistuksista vastaavat palveluntarjoajat. Opinnäytetyö ei ota kantaa kolmansiin osapuoliin.

4.7 Etäyhteydet ja palvelut

Yrityksellä ei ole toteutettuna etäyhteyksiä ja tai niihin liittyviä palveluita.

Yrityksen palvelut ovat AinaComilta, Aditrolta ja viaInnoxilta. Analyysi ei ota kantaa kolmansien osapuolien tuottamiin palveluihin.

5 SUUNNITTELU

Tarkoituksena oli suunnitella yritykselle riittävän automatisoitu, helposti ylläpidettävä ja kehityskestävä ympäristö. Suunnitelman perustana käytettiin kappaleen kaksi teoriapohjaa, josta ilmenee oikeat tavat ja menetelmät toteuttaa ympäristön ratkaisut. Uusien laitteiden ja ohjelmistojen hankinnoista lähetettiin tarjouspyyntö etukäteen. (Liite 9)

Ympäristön päivitys suunniteltiin pääsiäiseksi 2014, jolloin muutoksien tekoon tarjoutui neljä päivää aikaa. Ensimmäisenä päivänä tarkoituksena oli replikoida kaikki data SRV1:n ja SRV2:n välillä sekä varmistaa tiedot nauhalle. Tämän jälkeen molemmilta palvelimilta suunniteltiin ajettavaksi alas kaikki roolit ja palvelimien poisto domain-ympäristöstä. Näin ollen entinen forest olisi tuhottu ja voitiin tehdä uusi. Seuraavaksi suunniteltiin asennettavaksi uusi palvelin MTSrv01 ja kaikki sen roolit. Luotavaksi tuli uusi forest ja domain nimeltään TTMAKELA.LOCAL. Lopuksi aktivoitaisiin tarvittavat palvelimen omat monitorointityökalut käyttöön niiltä osin kuin ne olisivat tarpeellisia. Lisäksi uusi palomuuri tuli asentaa perusasetuksin.

Toisena päivänä suunniteltiin tarkastettavaksi palvelimelta ja palomuurilta lokit, jotta voitiin varmistua toimivuudesta. Toimivuuden toteamisen jälkeen tuli siirtää SRV1:ltä kaikki tiedostot MTSrv01:lle, jolle tehtäisiin samassa yhteydessä uudenlainen kansiorakenne. SRV1 kaavailtiin formatoitavaksi kokonaan, minkä jälkeen tuli asentaa uusi käyttöjärjestelmä, liittää se uuteen domainiin ja asentaa kaikki roolit. Nimeksi muodostui MTSrv02. Lisäksi palvelimelle suunniteltiin asennettavaksi ohjelmistot PRTG ja Spiceworks laajempaa monitorointia sekä valvontaa varten. Spiceworks toimisi myös Asset-tietokantana keräten tietoa ympäristön laitteista ja ohjelmistoista. Työasemien asennus tuli aloittaa ottamalla käyttöön ja asentamalla uudet työasemat sekä liittämällä ne uuteen domainiin.

Kolmantena päivänä suunniteltiin asennettavaksi loput työasemat. Koska kyseessä oli jo käytössä olleet koneet, tuli ne formatoida kokonaan asennuksen yhteydessä. Asennuksen jälkeen koneet liitettäisiin toimialueeseen. Kun palvelimien ja työasemien toimivuus olisi todettu, luotaisiin GPO:t ja aloitettaisiin ohjelmistojen jakelu.

Neljäntenä päivänä suunniteltiin jatkettavaksi ohjelmistojakelut loppuun ja tarkastettavaksi koko ympäristö sekä konfiguroida palomuurin asetukset niiltä osin mitä tarpeita vielä ilmenisi.

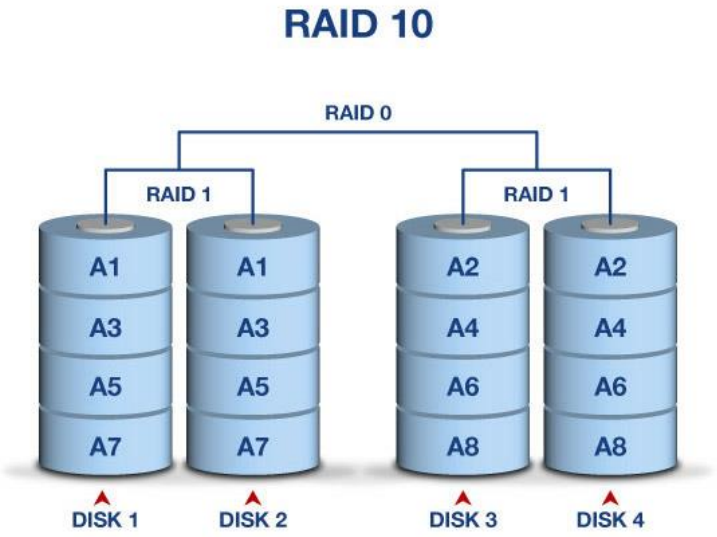
Toimeksiantajan toiveesta yksityiskohtaista suunnitelmaa ei sisällytetty opinnäytetyöhön. Kappaleessa 6 käsitellään kuitenkin koko ympäristön toteutus yleispiirteittäin niiltä osin kuin se toimeksiantajalle sopi.

6 TOTEUTUS JA TESTAUS

Toteutus ja testaaminen suoritettiin niin sanotulla big bang -menetelmällä eli infrastruktuuri muutettiin yhdellä kertaa. Etukäteen oli tiedossa, että koko ympäristö voitiin tehdä kokonaan uudestaan ja oli mahdollista aloittaa puhtaalta pöydältä. Infrastruktuurin muutos suoritettiin pääsiäisenä 2014.

6.1 Palvelimet

Toimeksiantajan toiveena oli ollut luopua vanhasta SRV2-palvelimesta. Näin ollen suunnitelman mukaan palvelin ajettiin alas ja poistettiin käytöstä. Tilalle hankittiin uusi palvelin, jotta palvelut pysyivät kahdennettuina. Lisäksi palvelimiin hankittiin uusi käyttöjärjestelmä Microsoft Windows Server 2012 R2 Standard. Kriteereinä uudella palvelimella olivat riittävä tehokkuus ja laajennettavuus myös tulevaisuutta ajatellen sekä toimiva varmistus. Fyysistä vikasietoisuutta parannettiin siirtymällä Raid 10 -tekniikkaan (Kuva 22). Laitteiden hankintaa koskeva tarjous on esitelty liitteessä 10.



Kuva 22. Uuden palvelimen Raid-tekniikka

Uudesta palvelimesta tehtiin primääri palvelin, joka hoitaa suurimman osan toiminnasta. Vanhasta palvelimesta tehtiin toissijainen, jolloin kriittisimmät palvelut pysyivät kahdennettuina. Palvelimet nimettiin uudelleen. Uudesta palvelimesta tuli MTSrv01 ja vanhasta MTSrv02. MTSrv01-palvelimelle asennettiin seuraavat roolit:

- AD DS
- DNS
- File and Storage Services
- IIS
- Print Services
- WDS
- WSUS.

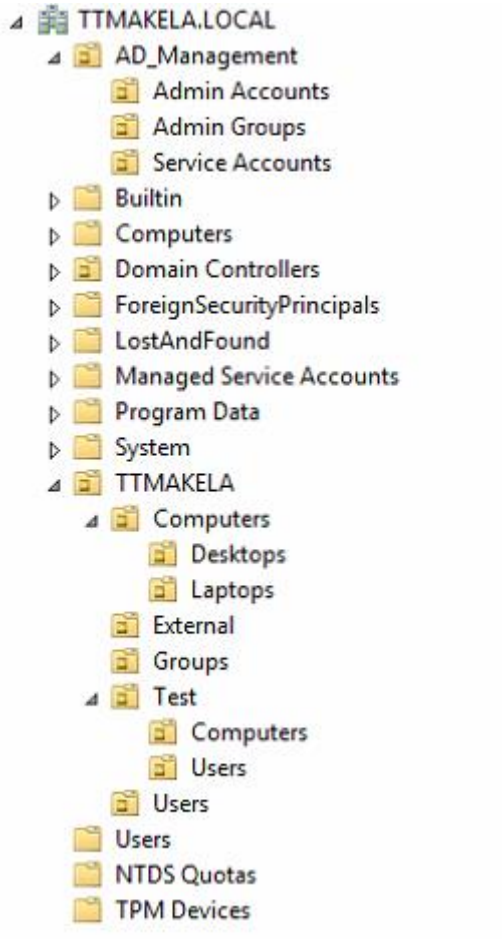
MTSrv02-palvelimelle asennettiin roolit:

- AD DS
- DNS
- File and Storage Services
- IIS.

MTSrv01:lle asennettiin lisäksi SQL-tietokanta Symantecin nauhavarmistusohjelmistoa varten. MTSrv02:lle asennettiin myös SQL-tietokanta wordpress, spiceworks ja prtg -ohjelmille.

6.1.1 Active Directory

AD:n rakenne luotiin kokonaan uudestaan vastaamaan parhaita menetelmiä. Huomioon otettiin myös mahdollisimman monipuolinen hallittavuus, selkeys sekä tarvittaessa mahdollisuus laajentaa yrityksen laitteistoa ja käyttäjistöä.



Kuva 23. Uusi AD-rakenne

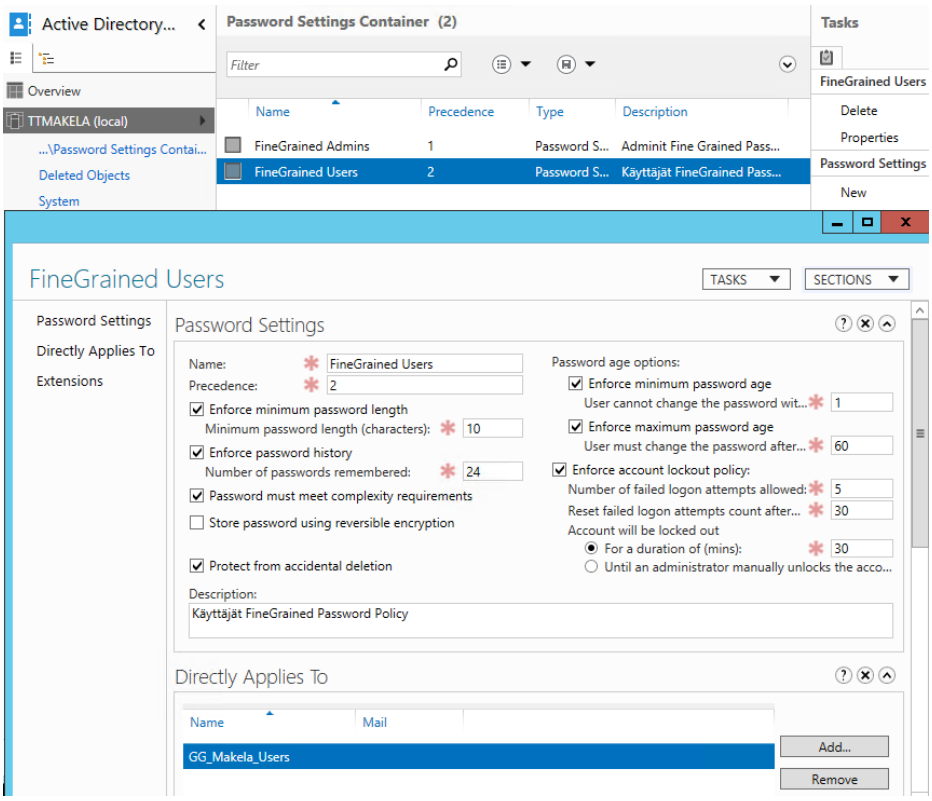
Active Directorylle luotiin kokonaan uusi forest ja domain nimeltä TTMAKELA.LOCAL. AD:n juureen luotiin hallintaa varten OU AD_Management, jonne tehtiin kolme alemman tason OU:ta. Näihin sijoitettiin Admin-tunnukset ja -ryhmät sekä palvelutunnukset. Käyttäjä- ja työasematileille luotiin AD:n juureen OU TTMAKELA ja sille ali-OU:t,

joihin sijoitettiin kaikki käyttäjät, työasemat ja ryhmät. Lisäksi tehtiin omat OU:t testausta ja ulkoisia käyttäjiä varten. AD:n rakenne näkyy kokonaisuudessaan kuvassa 23.

Advanced Audit Configuration	
Account Logon	
Policy	**Setting**
Audit Credential Validation	Success, Failure
Account Management	
Policy	**Setting**
Audit Computer Account Management	Success, Failure
Audit Other Account Management Events	Success, Failure
Audit Security Group Management	Success, Failure
Audit User Account Management	Success, Failure
Detailed Tracking	
Policy	**Setting**
Audit Process Creation	Success
DS Access	
Policy	**Setting**
Audit Directory Service Access	Success, Failure
Audit Directory Service Changes	Success, Failure
Logon/Logoff	
Policy	**Setting**
Audit Logoff	Success
Audit Logon	Success, Failure
Audit Special Logon	Success
Policy Change	
Policy	**Setting**
Audit Audit Policy Change	Success, Failure
Audit Authentication Policy Change	Success
Privilege Use	
Policy	**Setting**
Audit Sensitive Privilege Use	Success, Failure
System	
Policy	**Setting**
Audit IPsec Driver	Success, Failure
Audit Security State Change	Success, Failure
Audit Security System Extension	Success, Failure
Audit System Integrity	Success, Failure

Kuva 24. AD:n auditoinnin asetukset

AD:n auditoinnin (Kuva 24) lisäksi tietyt tapahtumat luokiteltiin monitorointiin seurattavaksi. Microsoft 2013a. luokittelee potentiaalisen kriittisyyden perusteella erinäiset tapahtumat ja seurattavaksi asetettiin sen perusteella korkeimman riskin omaavat tapahtumat 4618, 4649, 4719, 4765, 4766, 4794, 4897, 4964 ja 5124. Edellä mainituista tapahtumista sekä auditoinnin tapahtumista asetettiin monitorointiin asennettu ohjelmisto Spiceworks lähettämään sähköpostia järjestelmänvalvojille. Salasanojen hallinta toteutettiin myös AD:n avulla käyttäen Fine Grained -menetelmää (Kuva 25).



Kuva 25. Käyttäjien salasanapolitiikka

AD:n asennus ja konfigurointi suoritettiin Microsoftin parhaiden menetelmien mukaan (Liite 4) ja suojaaminen Microsoft 2013a. mukaan. Palvelun ollessa kriittinen asennettiin se kummallekin palvelimelle.

6.1.2 Tulostus (Print Services)

Yrityksellä on kolme verkkotulostinta, joita hallinnoidaan palvelimelta. Windows Server 2012 R2 tarjoaa uudentyyppisen universaaliin Type 4 -ajurin, joka asennettiin tulostinkohtaisesti MTSrv01-palvelimelle ja näin ollen koko tulostuspalvelu on asennettuna yhdellä palvelimella. Osaa tulostimien ominaisuuksista ei kuitenkaan pystytä uudenlaisilla ajureilla hallitsemaan, joten palvelimelle asennettiin myös vanhemmat laitekohtaiset Type 3 –ajurit (Kuva 26).

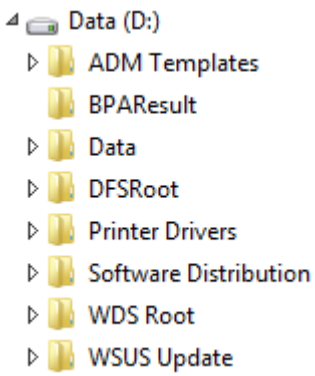
Lähetä OneNote 2010:een	Ready	0	MTSrv01 (local)	Send To Microsoft OneNote 2010 ...	
Microsoft XPS Document Writer	Ready	0	MTSrv01 (local)	Microsoft XPS Document Writer v4	6.3.9600.16384
RICOH 2045e	Ready	0	MTSrv01 (local)	RICOH Class Driver	6.3.9600.17415
RICOH 4502 PCL6 UniversalDriv...	Ready	0	MTSrv01 (local)	RICOH PCL6 UniversalDriver V4.3	4.3.0.0
RICOH 5000 PCL6 UniversalDriv...	Ready	0	MTSrv01 (local)	RICOH PCL6 UniversalDriver V4.3	4.3.0.0
RICOH MP C4502	Ready	0	MTSrv01 (local)	RICOH Class Driver	6.3.9600.17415
RICOH MP C5000	Ready	0	MTSrv01 (local)	RICOH Class Driver	6.3.9600.17415
RICOH v4 type3	Ready	0	MTSrv01 (local)	RICOH Class Driver	6.3.9600.17415

Kuva 26. Tulostuspalvelu

Tulostuksen hallinnan asennus ja konfigurointi suoritettiin Microsoft 2012a. mukaan.

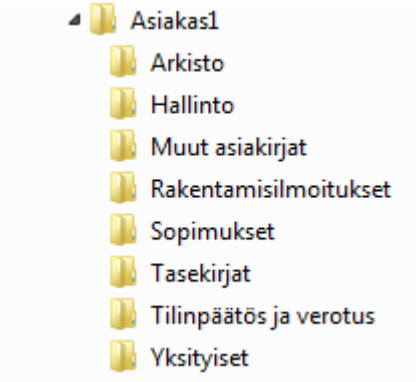
6.1.3 File and Storage Services

Käyttäjille näkyvät päätason jaot määritettiin olevaksi D:\DFS, jossa sijaitsee kaikki verkossa oikeuksien mukaan jaettava tieto ja D:\Data, jossa kotihakemistot sijaitsevat.



Kuva 27. Uusi kansiorakenne

Lisäksi luotiin kansiot keskitetyille päivityksille, käyttöjärjestelmien asennuksille, ohjelmistojakeluille, tulostinajureille ja ryhmäkäytäntöjen malleille (Kuva 27). DFSRoot-kansioon tehtiin alikansioiksi asiakkaat, IT, Johto, Pankki ja Yhteinen ja niistä tehtiin piilotetut kansiot lisäämällä $-merkki jakoresurssin nimen perään. Asiakkuuksia koskevat kansiot luotiin uudenlaisella rakenteella, johon kaikki data siirrettiin. Kansiorakenne vastaa Taloushallintoliiton suosituksia soveltaen (Kuva 28).



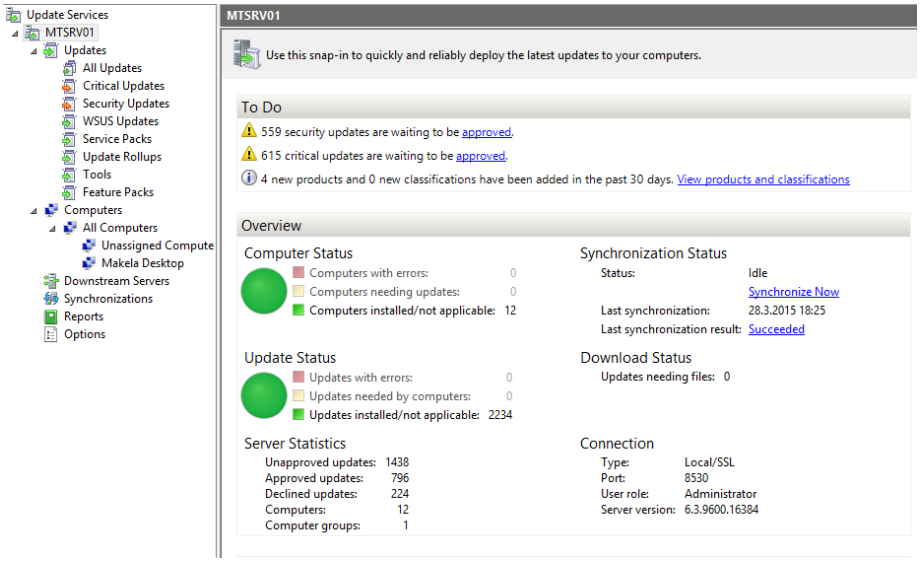
Kuva 28. Asiakaskansion rakenne

D:\DFSRoot-jakoon ja sen alikansioihin määritettiin oikeudet käyttäjällä olevan AD-ryhmän relaatiolla ryhmäkäytäntöön. Verkkoresurssien yhdistäminen näin ollen tapahtuu GPO:lla, jota käsitellään tarkemmin kohdassa 5.1.6. Palvelimen D-asemalle otettiin käyttöön Shadow Copy toiminto, joka toteutettiin Microsoftin parhaiden menetelmien mukaan. (Microsoft 2013b.)

6.1.4 WSUS (Windows System Update Services)

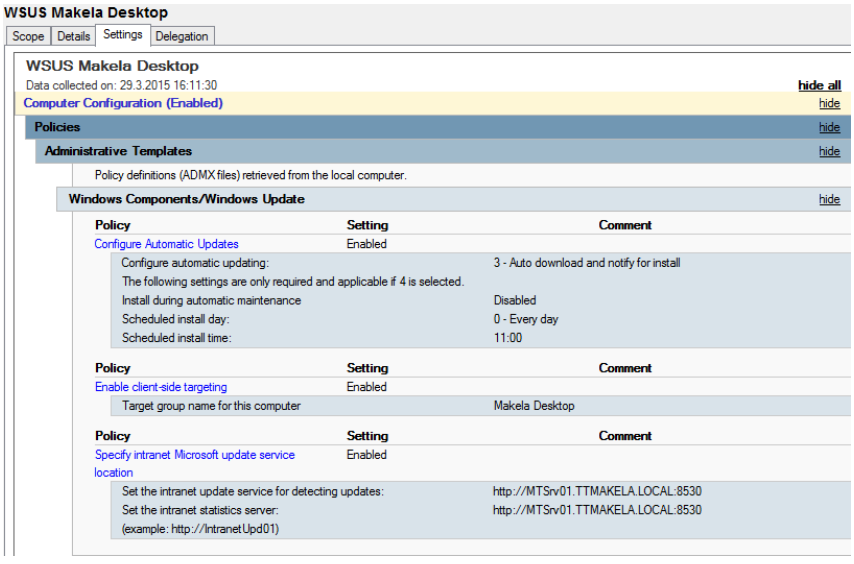
WSUS-rooli asennettiin MTSrv01-palvelimelle ja siihen kuuluvat WID Database ja WSUS Services -palvelut (Kuva 29). Päivitysten varastoimi-

seen osoitettiin palvelimelta resurssi D:\WSUS\. Palvelin määritettiin primääriksi, joka synkronoi mahdolliset Microsoftin julkaisemat päivitykset kerran vuorokaudessa. Lisäksi määritettiin, mihin käyttöjärjestelmiin ja ohjelmistoihin päivityksiä haetaan sekä millaisen luokituksen omaavia päivityksiä synkronoidaan.



Kuva 29. WSUS päänäkymä

Palveluun luotiin ryhmä Makela Desktop, joka linkitettiin luotuun GPO:hon (Kuva 30). Asetukset tehtiin puoliautomaattisiksi siten, että WSUS tarkastaa päivitysten saatavuuden ja ilmoittaa uusista päivityksistä sähköpostitse järjestelmänvalvojille, jolloin kaikki päivitykset täytyy erikseen hyväksyä ladattavaksi ja asennettavaksi.

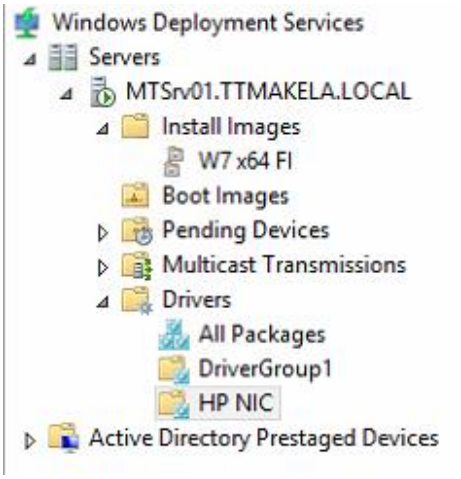


Kuva 30. WSUS GPO työasemille

Näin saatiin luotua kontrolloitu hallinta, jolloin kaikki asennettavat päivitykset voidaan ensin tarkastaa ennen kuin ne määritellään työasemille asennettaviksi. WSUS:n asennus ja konfigurointi suoritettiin Microsoft 2014c.:n mukaan.

6.1.5 WDS (Windows Deployment Services)

WDS-rooli asennettiin MTSrv01-palvelimelle ja sille määritettiin resurssiksi D:\WDS Root. Asennettavan käyttöjärjestelmän levykuva kopioitiin osoitettuun resurssiin. Levykuvasta valittiin asennuskuva ja käynnistyskuva. Lisäksi määritettiin palvelulle käynnistyksen yhteydessä määräytyvät ja latautuvat verkkokortin ajurit (Kuva 31).



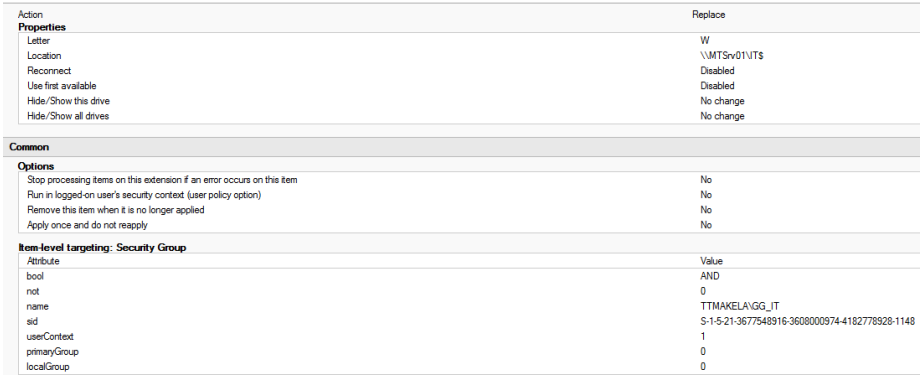
Kuva 31. WDS

6.1.6 GPO (Group Policy Object)

Ryhmäkäytännöt jaoteltiin kahteen osaan, työasemakohtaisiin ja käyttäjäkohtaisiin. Työasemille kohdennettuihin käytäntöihin luotiin hierarkiassa ylimmäksi GPO, joka odottaa verkon vastaavan aina, kun tietokone käynnistetään ja siihen kirjaudutaan. Näin ollen kaikki verkon kautta asetetut asetukset saatiin varmasti aina aktiivisiksi. Muita työasemiin kohdistuvia ryhmäkäytäntöjä luotiin seuraavasti:

- DNS:n PTR tunnisteen automaattinen luonti
- Viimeisen kirjautumisen piilotus työaseman näytöltä
- Auditointi
- Työasemakohtaisen palomuurin ja virrankäytön asetukset
- WSUS:n tarvitsema GPO
- Chrome ja firefox –selainten asetukset
- RPC asetukset
- Laitteiden ja ohjelmistojen asentamisen automatisointiin liittyvät GPO:t.

Käyttäjäkohtaisia ryhmäkäytäntöjä luotiin huomattavasti vähemmän. Niillä rajattiin muun muassa sitä, mitä komponentteja käyttöjärjestelmästä näkyy käyttäjille ja mitä laitteita voidaan asentaa ilman järjestelmänvalvojan oikeuksia. Lisäksi määritettiin tiedostopäätteiden näkyvyys.

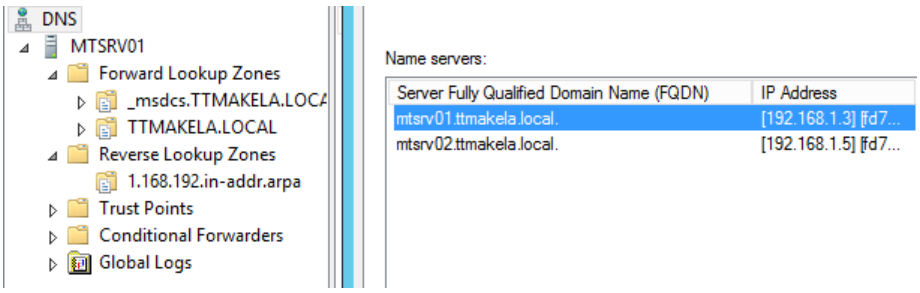


Kuva 32. GPO esimerkki verkkoresurssin yhdistämisestä

Toiminnallisuudeltaan merkittävin GPO luotiin yhdistämään käyttäjille verkkolevyt. Kappaleessa 6.1.3 esitetyn kansiorakenteen mukaan luotiin viisi eri AD-ryhmää vastaamaan kansion nimeä, esimerkiksi GG_IT, jolla oikeudet annettiin kyseiseen kansioon. AD-ryhmä linkitettiin ryhmäkäytäntöön, jolloin lisättäessä käyttäjälle esimerkin ryhmä, yhdistyi kyseinen levyresurssi (Kuva 32). Näin saatiin automatisoitua levyresurssien yhdistyminen tietyin halutuin oikeuksin. Tämä yhdistettynä kansion näkyvyyteen saatiin verkkoresurssien tarkastelu estettyä, kun oikeuttavaa AD-ryhmää ei ole käytössä. Ryhmäkäytännöt on osin esiteltynä liitteessä 11.

6.1.7 DNS (Domain Name Services)

DNS-palvelu asentuu AD:n asennuksen yhteydessä, joten sitä ei varsinaisesti erikseen asennettu. Palvelu konfiguroitiin siten, että luotiin Active Directory integroidut vyöhykkeet. Vyöhykkeille asetettiin turvatut dynaamiset päivitykset ja niiden siirto sallittiin vain MTSrv01:n ja MTSrv02:n välillä (Kuva 33).



Kuva 33. DNS palvelun yleisnäkymä ja nimipalvelimet

Käänteisen nimihaun vyöhyke (Reverse Lookup Zone) tuli tehdä ja määrittää manuaalisesti. Vyöhykkeelle tulevat tiedot asetettiin toimimaan työasemiin kohdistetulla GPO:lla seuraavin määrityksin:

- Register DNS records with connection-specific DNS suffix Enabled
- Register PTR records Enabled
- Register PTR records: Register only if A record registration succeeds.

Palvelun tietueiden tietojen vanhenemisajaksi asetettiin seitsemän vuorokautta, mikä vastaa Microsoftin parhaita menetelmiä. Palvelun toimiessa päälähteenä nimihaulle yrityksen koko ympäristössä, asetettiin sille myös

riittävästi ulkoisia nimipalvelimia, joihin kyselyt voitaisiin ohjata (Kuva 34). Juuripalvelimet tarkastettiin ja DNS-palvelusta poistettiin kaikki ne, jotka eivät kyselyihin vastanneet.

IP Address	Server FQDN
81.16.78.3	ns2.tko.fi
213.140.164.26	ns2.it.tko.fi
212.149.120.42	ns.tko.fi
8.8.8.8	google-public-dns-a.google.com

Kuva 34. DNS Forwarders

Projektin aikana päätettiin toimeksiantajan kanssa siirtää DNSSEC:n käyttöönotto myöhemmälle ajankohdalle ja näin ollen se rajattiin projektin ulkopuolelle. Palvelun asennus ja konfigurointi suoritettiin noudattaen parhaita menetelmiä, jotka ovat esiteltynä liitteessä 5.

6.2 Työasemat

Yrityksen laitteisto työasemien osalta oli varsin hyvä. Kuitenkin viisi konetta oli tullut tiensä päähän, joten ne uusittiin tarjouksen perusteella (Liite 10). Näin ollen päädyttiin laitteistollisesti kahteen erityyppiseen työasemaan, vanhoihin ja uusiin (Fujitsu ja Hewlett-Packard), jotka erosivat ainakin ajuriensa osalta. Työasemille luotiin yksi OU, johon ne voitiin kaikki sijoittaa, koska eroavaisuudet eivät merkinneet vaikuttavasti ryhmäkäytäntöjen asetuksiin.

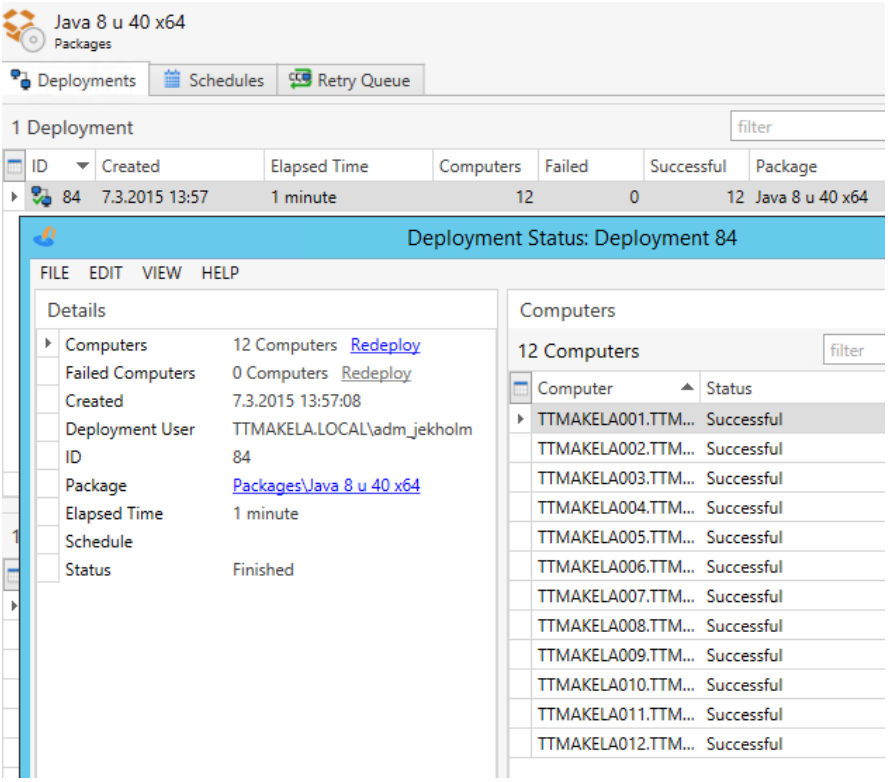
Työasemat asennettiin käyttäen levykuvaa, joka sijaitsi MTSrv01-palvelimella. Koneiden kiintolevyt alustettiin asennuksen yhteydessä ja kaikki työasemat asennettiin samoin asetuksin. Ohjelmistojen jakeluun käytettiin PDQ Deploy -ohjelmaa, jolla voitiin asennukset suorittaa keskitetysti ja yhdellä kertaa (Kuva 35). Ajureiden ja BIOS:n hallinnointiin ja päivityksiin käytettiin kyseisen tai kyseisten valmistajien omaa päivitystyökalua.

6.2.1 Työasemavakio

Käyttöjärjestelmänä työasemiin asennettiin Windows 7 Pro SP1 64-bit. Vakio koostui seuraavista ohjelmista jotka asennetaan työasemiin:

- Mozilla Firefox
- Java 8
- Adobe Reader
- Adobe Flash
- Unes
- Google Chrome
- PDF Creator
- PDF Architech
- CutePDF
- F-Secure Client Security
- Microsoft Silverlight

- Microsoft Office 2013 Home & Business
- Citrix Reciever
- Visio Viewer 2010
- KeePass.

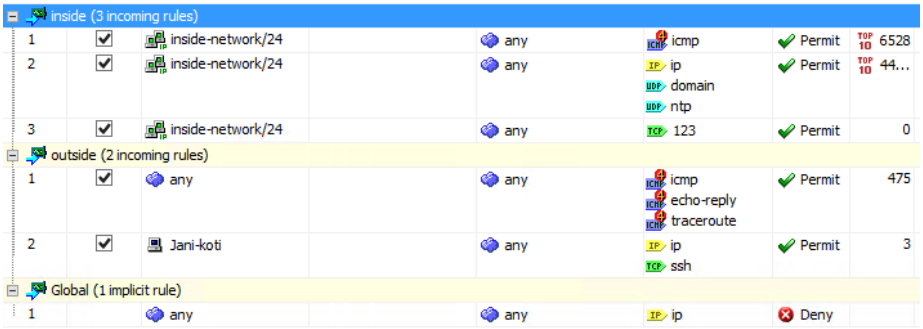


Kuva 35. Esimerkki ohjelmiston jakelusta

Toimeksiantajan kanssa sovittiin, että työasemavakio tarkastetaan puolivuosittain ja tarvittaessa kokoonpano ohjelmistollisesti muutetaan.

6.3 Lähiverkko

Lähiverkon osalta muutoksia ei juurikaan tarvinnut tehdä. Vanhentuneen palomuurin tilalle hankittiin uusi laite, Cisco ASA 5505. Uudelle palomuurille määritettiin ulkoverkkoon yksi kiinteä IP-osoite yrityksen julkisten IP-osoitteiden avaruudesta. Sisäverkon laitteiden osoitteet asetettiin käyttämään ulkoverkkoon näkyvää osoitetta NAT:n avulla. Sisäverkosta ulospäin sallittiin IP- ja ICMP-liikenne osoitteista riippumatta. Lisäksi sallittiin palvelinten tarpeeseen domain- ja NTP-liikenne sekä avattiin kokonaisuudessaan portti 123. Ulkoverkosta sisäverkkoon sallittiin ainoastaan SSH- ja IP-liikenne tietyistä IP-osoitteista (Kuva 36). Palomuuri konfiguroitiin perustoiminnoiltaan liitteen kolme mukaisesti. Muu konfiguraatio suljettiin ulos opinnäytetyöstä toimeksiantajan pyynnöstä arkaluontoisten asetusten johdosta.

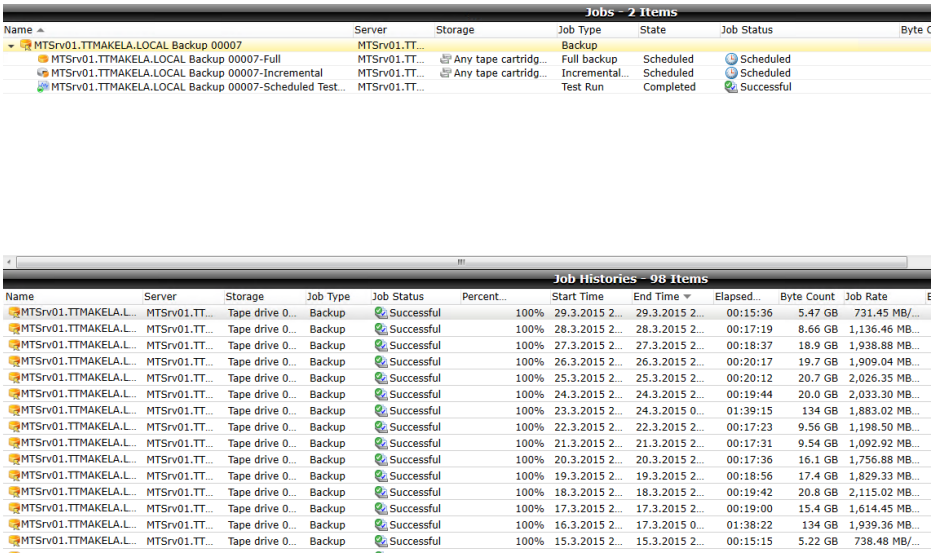


Kuva 36. Palomuurin liikenteen säännöt

Yritykselle luotiin myös IPv6-lähiverkko tulevaisuuden varalle, mutta sitä ei varsinaisesti otettu käyttöön. Palvelimille asetettiin IPv6-osoitteet, mutta kaikille muille laitteille ne jätettiin laittamatta.

6.4 Varmistukset

Uuden palvelimen varusteeksi tilattiin uusi nauhavarmistin ja 5 nauhaa. Varmistukset toteutettiin siten, että määritettiin neljä nauhaa käytettäväksi aina yksi viikon kerrallaan. Nauhalle tallennettiin kaikki tieto MTSrv01-palvelimesta maanantaisin. Muina päivinä nauhalle varmistuivat vain muuttuneet tiedot. Viides nauha osoitettiin niin sanotuksi kuukausinauhaksi, johon varmistettiin koko ympäristö aina kuun viimeisenä päivänä. Näin saatiin luotua looginen rotaatio nauhojen kanssa, mikä osoittautui myös yritykselle hyväksi käytännöksi. Ohjelmistona toimi Symantec Backup Exec 2014 (Kuva 37).



Kuva 37. Nauhavarmistus

Yritykselle tärkeän taloushallinnon ohjelmiston tietojen varmistukset tallennettiin DVD-levylle ja jatkossakin toimeksiantaja tulee samalla lailla toimimaan. Muilta osin kolmansien osapuolten tuottamien palveluiden varmistukset rajattiin pois opinnäytetyöstä.

6.5 Etäyhteydet, palvelut ja sähköpostijärjestelmät

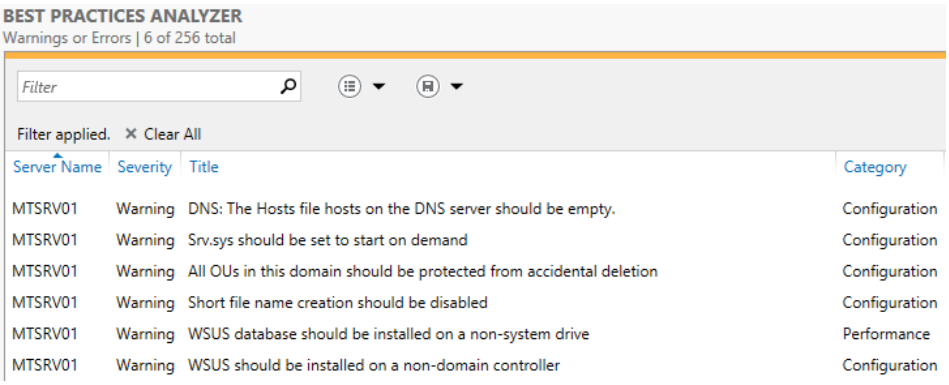
Toimeksiantaja ei katsonut tarpeelliseksi avata käyttäjille etäyhteyksiä yrityksen verkkoon. Hallinnointia varten kuitenkin avattiin VPN- ja SSH-yhteydet. SSH:lle määritettiin tietyt IP–osoitteet, joista yhteys sallitaan. VPN toteutettiin Ciscon AnyConnect-periaatteella, jossa yhteys muodostetaan käyttäen Ciscon omaa sovellusta. Lopulta yrityksen johto kiinnostui VPN-yhteyden mahdollisuuksista ja halusi toiminnan testattavakseen.

Kolmansien osapuolten toimittamat palvelut rajattiin opinnäytetyön ulkopuolelle. Palvelut kuitenkin pysyivät käytössä sellaisinaan kun ne olivat.

7 MONITOROINTI JA AUDITOINTI

Monitorointiin ja auditointiin käytettiin useampaa ohjelmistoa, jotta mahdollisten virheiden ja epäkohtien seurannasta saatiin kattava ja luotettava kokonaiskuva. Ohjelmistot asennettiin MTSrv02-palvelimelle. Ohjelmistojen lisäksi käytettiin palvelinten omia lokeja ja analysointityökaluja.

Asetusten ja toiminnallisuuden tarkastamiseen käytettiin Microsoftin Best Practices Analyzer -työkalua. Sovellus skannaa palvelimen ja sen roolit sekä asetukset ja vertaa niitä valmistajan tietokannassa oleviin sääntöihin (Kuva 38).



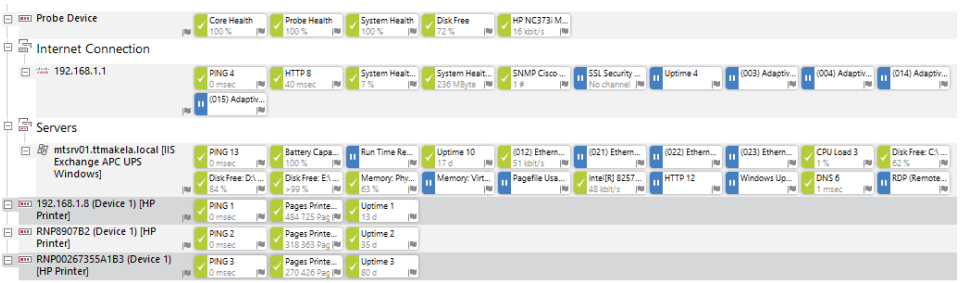
Kuva 38. BPA-skannaus

Skannauksen jälkeen tarkastettiin tulokset ja tehtiin tarvittavat toimenpiteet varoitusten ja virheiden korjaamiseksi. WSUS:iin liittyvät virheet jätettiin huomioimatta, koska yrityksellä oli käytössään vain kaksi palvelinta. Näin ollen roolille ei ollut mahdollista osoittaa omaa palvelinta. Lisäksi tiedostopalvelimen varoituksia tutkittiin Microsoftin tukisivustoilta. Johtopäätöksenä päädyttiin tulokseen, että virheet ohitetaan, koska niiden korjaaminen oli aiheuttanut lukuisille muille ylläpitäjille ongelmia palvelimen toiminnassa.

7.1 PRTG

Verkon ja laitteiden yleisen toiminnan valvomiseen käytettiin PRTG-ohjelmistoa. Sovellus käyttää hyväkseen SNMP, SSH, WMI tai NetFlow -

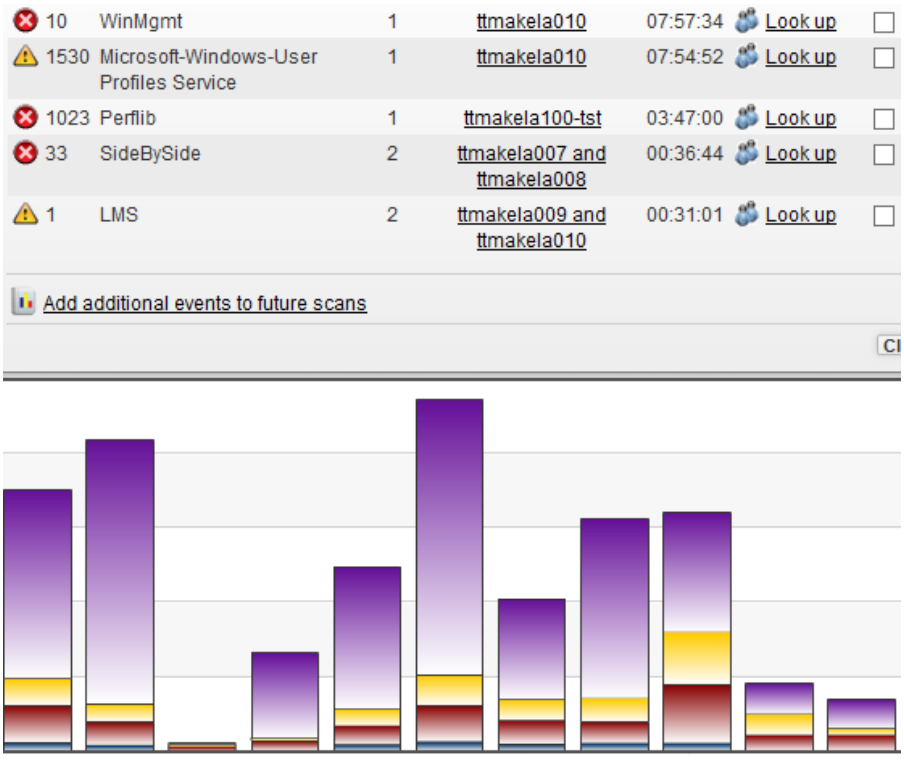
tekniikka luodatakseen laitteita ja laitteiden sensoreita. Sovelluksen avulla valvottiin palvelinten, tulostimien ja palomuurin kriittisiä toimintoja yleisellä tasolla (Kuva 39). Ohjelmalle asetettiin tietyt rajat jokaiseen valvottavaan objektiin ja mikäli rajat rikkoutuisivat, lähetettäisiin siitä sähköpostitse ilmoitus järjestelmänvalvojille.



Kuva 39. PRTG toiminnassa

7.2 Spiceworks

Yksityiskohtaisempaan monitorointiin käytettiin Spiceworks-ohjelmaa. Sovelluksella skannattiin yrityksen käytössä oleva sisäverkon segmentti, minkä jälkeen ohjelma kokosi laitteista luettelot ja luokitteli ne roolinsa mukaan. Laajojen ominaisuuksien vuoksi Spiceworks sopi hyvin työkaluksi toimeksiantajan ympäristön valvontaan. Ohjelma myös lukee palvelinten ja työasemien tapahtumalokia perustuen GPO:lla asetettuihin auditointiasetuksiin, joten erillistä ohjelmaa ei siihen tarkoitukseen tarvinnut enää asentaa (Kuva 40).

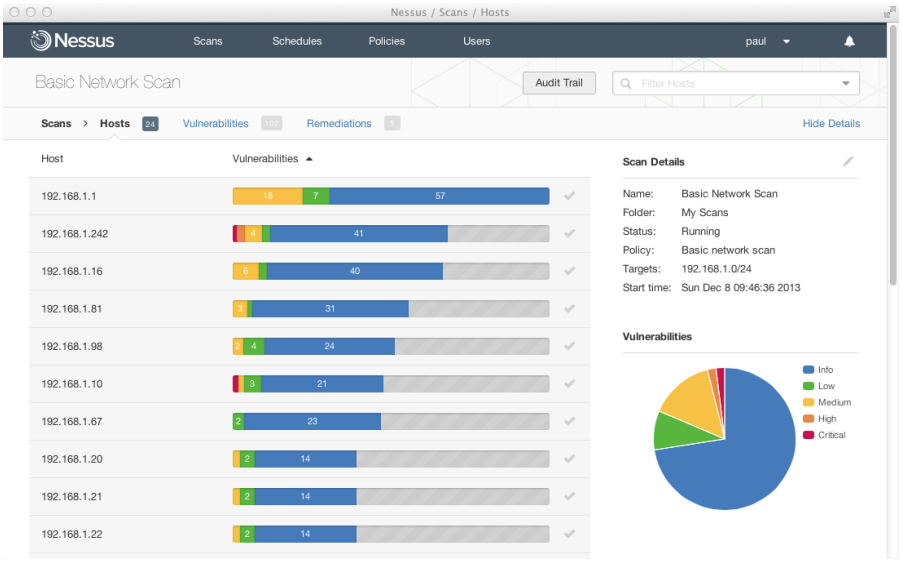


Kuva 40. Spiceworks-toimintoloki ympäristön laitteista

Sovellus konfiguroitiin lähettämään ilmoitus järjestelmänvalvojille sähköpostitse, mikäli ennalta-asetut kriteerit virheiden suhteen täyttyivät. Menetelmä osoittautui varsin hyväksi, eikä erillistä lokien tutkintaa laitekohtaisesti tarvinnut juurikaan suorittaa.

7.3 Linux

Linuxia käytettiin myös apuvälineiden alustana monitorointiin. Tietoturvan osalta työkaluna käytettiin Nessus-sovellusta, jolla tutkittiin koko ympäristön kaikki laitteet mahdollisten tietoturva-aukkojen varalta. Ohjelma skannasi laitteet hyödyntäen kaikkia tunnettuja penetraatiomenetelmiä ja haavoittuvuuden hyödyntämisen tapoja. Tulosten perusteella voitiin olla tyytyväisiä laitekohtaiseen tietoturvaan (Kuva 41).



Kuva 41. Esimerkki Nessus-sovelluksen käytöstä

Palveluiden ja laitteiden saatavuuden laskentaan asennettiin Nagios. Sovelluksella mitattiin palvelinten ja palveluiden mahdollisia käyttökatkoja, minkä perusteella voitiin luoda kuvan 42 raportti. Tarkasteluaikana ei kuitenkaan käyttökatkoja esiintynyt, joten palveluiden saatavuus oli 100%.

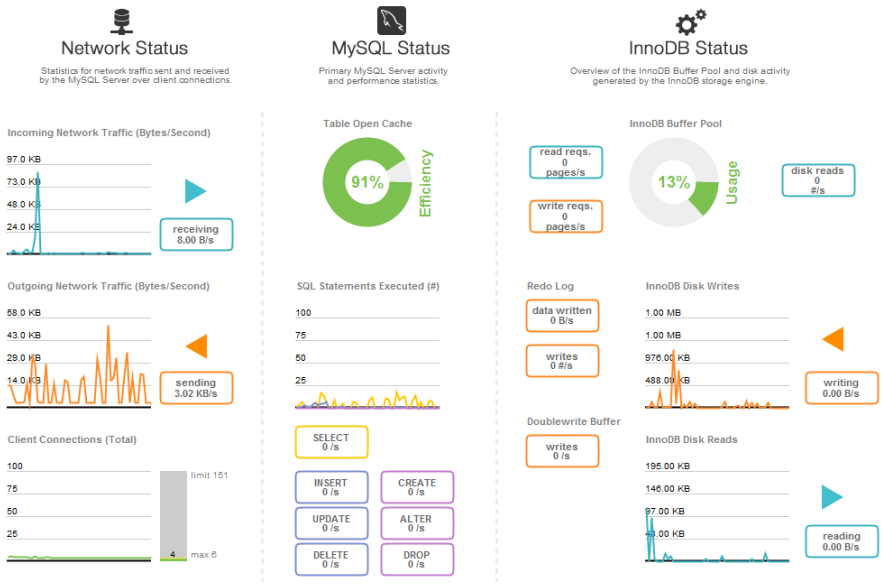
Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	45d 17h 53m 40s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	45d 17h 53m 40s	100.000%	100.000%
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	45d 17h 53m 40s	100.000%	100.000%

Kuva 42. Nagios-raportti MTSrv02-pavelimesta

7.4 SQL-kannat

SQL-kantojen toimintaa ja tehokkuutta valvottiin SQL Workbench -ohjelmalla (Kuva 43). Valvottavana oli verkon käyttö, tietokantojen kuormitus niin kirjoituksen kuin lukemisen osalta ja välimuistin käyttö. Käyttäjiä pyydettiin käyttämään Wordpress-ohjelmaa, jotta kuormitus saatiin mahdollisimman korkeaksi. Seurannan perusteella voitiin todeta SQL-kantojen hyvä toimivuus ja tehokkuus.



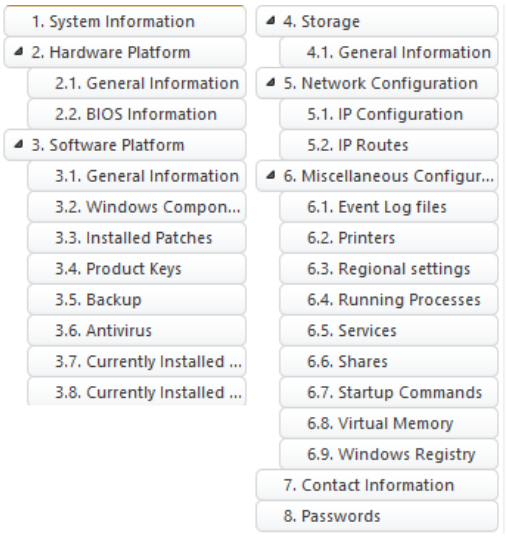
Kuva 43. SQL Workbench

8 TIETOTURVA

Toimeksiantajan toiveesta tietoturvaan liittyvät toteutetut asiat tuli jättää pois opinnäytetyön raportista. Tietoturvasuunnitelma haluttiin pitää salaisena, koska siinä on arkaluontoista tietoa yrityksen sisäisistä prosesseista ja menetelmistä. Tietoturvasuunnitelma luotiin yhdessä yrityksen johdon kanssa, jotta se voitiin suunnitella sovellettavaksi heidän tarpeisiinsa ja infrastruktuuriinsa. Suunnitelman teossa noudatettiin ISO 17799:2005 / ISO 27002:2005 standardia. Standardin perusteella luotu runko on esiteltynä liitteessä 12.

9 DOKUMENTOINTI

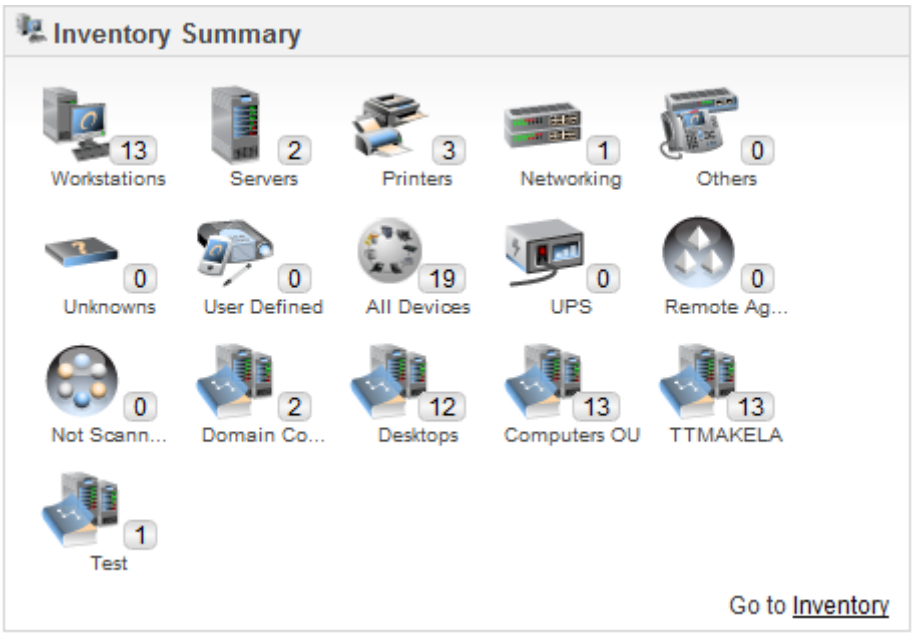
Yrityksen IT-infrastruktuurin dokumentointiin käytettiin kahta työkalua. Ensimmäisenä työkaluna käytettiin Sydi Server -skriptiä. Sydi Server kerää tiedot laitteesta kerrallaan perustuen skriptiin. Skripti kartoittaa laitteista tietoja muodostaen niistä Word-dokumentin (Kuva 44).



Kuva 44. Sydi Server -dokumentin sisällys

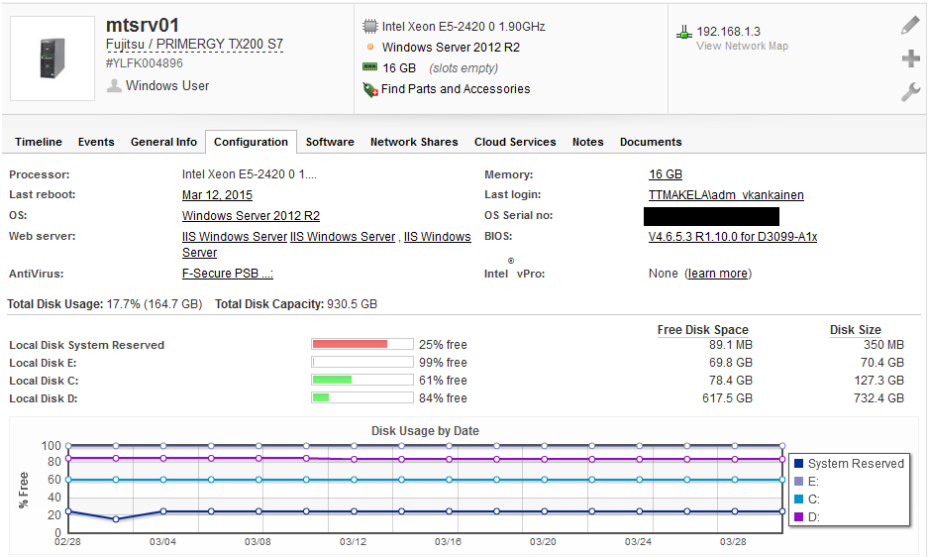
Skriptin avulla kartoitettiin ympäristön kaikki laitteet muodostaen niistä laitekohtaiset dokumentaatiot.

Spiceworks toimi toisena dokumentoinnin työkaluna. Sovelluksella skannattiin laitteista kaikki tieto käyttäen hyväksi toimialuetta (Kuva 45). Ohjelmalle annettiin riittävän vahvan tunnuksen oikeudet vastaamaan järjestelmänvalvojan oikeuksia.



Kuva 45. Verkon laitteet

Ohjelmaa hyödynnettiin myös soveltaen ITIL:n määrittämään CMS-järjestelmään. Spiceworks kerää ja varastoi kaiken tiedon laitteiden ohjelmistoista ja konfiguraatiosta sekä niiden muutoksista. Sovellus myös päivittää ja ylläpitää CMS-tietokantaansa automaattisesti havaittuaan muutoksia laitteissa ja sovelluksissa (Kuva 46).



Kuva 46. Yksityiskohtainen dokumentointi laitteesta

Opinnäytetyön raportin osalta dokumentointi rajattiin vain yleiselle tasolle. Tiedoissa oli paljon toimeksiantajalle salaista tietoa, joten yksityiskohtaisempi kuvaus koko IT-ympäristöstä rajattiin työn raportoinnin ulkopuolelle.

10 JOHTOPÄÄTÖKSET

Opinnäytetyön ajoitus osui yritykselle varsin hyvään aikaan. Microsoft lopetti kesällä 2014 tuen vanhalle XP-käyttöjärjestelmällä ja näin ollen toimeksiantajan tarve uusia ympäristö oli valtava. Etukäteen oli tiedossa myös se, että yrityksen palvelimet olivat vanhanaikaiset ja koko ympäristö oli suuren päivityksen tarpeessa.

Työn alussa toimeksiantajan IT-infrastruktuuri oli varsin sekava. Kartoitusta tehdessä eri järjestelmien ja konfiguraatioiden dokumentointia ei löytynyt, sitä ei ollut olemassakaan tai se oli puutteellista. Sisäisiin IT-prosesseihin ja tietoturvaan liittyvät asiat olivat alkeellisia tai olemattomia eikä niihin suhtauduttu riittävällä vakavuudella. Tämä ilmeni esimerkiksi siitä, että toimeksiantajalla ei ollut minkäänlaista suunnitelmaa tai politiikkaa tietoturvaan tai ylipäätään koko IT-ympäristöön liittyen, eikä käyttäjien oikeuksia ollut millään lailla rajattu. Nykyään kyseinen ilmiö on valitettavasti varsin yleinen suomalaisissa pk-yrityksissä.

Kartoituksen ja analyysin aikana havaitut puutteet ja epäkohdat saatiin korjattua ja kaikki tarvittavat laitteet sekä ohjelmistot uusittua. Yritykselle luotiin toimintaperiaatteet ja tekniikat, joilla laitteiden ja käyttäjien hallinta voitiin suorittaa keskitetysti ja tietoturvallisesti. Palvelimiin valittiin käyttöjärjestelmät, joiden tuki jatkuu vuoteen 2023. Työasemien käyttöjärjestelmien tuki jatkuu Microsoftin mukaan vuoteen 2020. Palomuurin osalta elinkaaren päättymispäivää ei ole vielä Ciscon toimesta julkistettu. Näin ollen ympäristön elinkaaren jatkuvuus turvattiin avainlaitteiden osalta. Lisäksi tietoturva ja sen suunnitelma sekä dokumentointi yrityksen IT-infrastruktuurista saatettiin vastaamaan standardeja ja asetuksia. Ympäris-

tö suunniteltiin ja toteutettiin myös siten, että tarvittaessa se on mahdollista siirtää osittain tai kokonaan pilveen. Lisäksi sen laajentamisen mahdollisuudet ovat merkittävät. Yhtenä suurimpana uudistuksena koko ympäristössä oli myös toteutettu mahdollisuus käyttäjille tehdä työnsä ajasta ja paikasta riippumatta. Projektin jälkeen voidaan periaatteessa puhua yrityksellä olevan hybridiympäristö, koska exchange-palvelut ja taloushallinnon ohjelmistot sijaitsevat kokonaan toisessa toimialueessa ja pilvessä.

Projektiluontoisissa töissä työn määrällä on usein taipumus paisua ulos alun perin suunnitelluista raameista. Koska kyseessä on reilun kymmenen henkilön yritys, IT-laitteita ei ollut paljon. Siitä huolimatta projektin aikana ilmeni aina vain uusia ja uusia tarpeita, jotka laajensivat alun perin suunniteltua opinnäytetyötä huomattavasti. Haasteena oli rajata projektiin sisällytettävät ja poisjätettävät kehityskohteet. Päätöksien vaikeutta lisäsi se, että toimeksiantajan toimesta kerrottiin mahdollisten lisätöiden olevan heille arvokkaita. Näin ollen yrityksen toiveita yritettiin toteuttaa ja sisällyttää työhön mahdollisimman paljon. Lisäksi projektia tehdessä opinnäytetyön tekijä havaitsi, kuinka tärkeää myös pienelle yritykselle on omata henkilö tai henkilöitä, joilla on kokonaiskäsitys IT-ympäristön tilasta ja hallinnasta. Tilanteessa, jossa kukaan ei ole kokonaan vastuullinen tai tietoinen IT-infrastruktuurista, voidaan ajautua tilanteeseen, joka toimeksiantajalla valitettavasti oli opinnäytetyön alkuvaiheessa.

Tämän opinnäytetyön tulokset ovat lähestulkoon poikkeuksetta kenen tahansa käytettävissä. Microsoftin tuotteet ja tietoturva-asiat ovat yleisimpiä seikkoja missä tahansa IT-ympäristössä. Lisäksi ITIL on yhä useamman yrityksen käytössä linjaamassa IT:n johtamista prosessein ja yleinen käytäntö on, että kuka tahansa voi käyttää ITIL:iä.

Opinnäytetyön suorituksen myötä toimeksiantajan tietoisuus IT:n tärkeydestä apuvälineenä yrityksen toiminnalle kasvoi merkittävästi. Yrityksen johto on tullut tietoiseksi IT-ympäristöstä ja sen laitteista ja mahdollisuuksista hyödyntää IT-infrastruktuuria paremman tuloksen ja tyytyväisyyden saavuttamiseksi. Projektin myötä toimeksiantaja on tiedostanut myös ylläpidon merkityksen ja tärkeyden ja halunnut jatkaa yhteistyötä opinnäytetyön tekijän kanssa. Opinnäytetyön suorittamisen jälkeen yrityksellä on käytössään ajantasainen, tietoturvallinen ja moderni IT-infrastruktuuri ja se vastaa taloushallintoliiton auktorisoidulle yritykselle asetettuihin vaatimuksiin.

LÄHTEET

Cisco 2012. Internetworking Technology Handbook. Viitattu 22.1.2015. http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook

Cisco. n.d.a. Cisco Firewall Best Practices Guide. Viitattu 22.1.2015 http://www.cisco.com/web/about/security/intelligence/firewall-best-practices.html#_Toc332806023

ISO/IEC27002:2005. 2005. Information technology – Security techniques – Code of practice for information security management. Viitattu 12.11.2014.

Microsoft. 2010. Best Practices Analyzer for Domain Name System. Viitattu 10.1.2015. https://technet.microsoft.com/en-us/library/dd391963%28v=ws.10%29.aspx

Microsoft. 2010a. Best Practices Analyzer for File Services. Viitattu 20.2.2015. https://technet.microsoft.com/en-us/library/ff633443%28v=ws.10%29.aspx

Microsoft. 2011. Group Policy for Beginners. Viitattu 23.8.2014 https://technet.microsoft.com/en-us/library/hh147307%28v=ws.10%29.aspx

Microsoft. 2011a. Best Practices Analyzer for Windows Server Update Services. Viitattu. 11.12.2014. https://technet.microsoft.com/en-us/library/ff646957%28v=ws.10%29.aspx

Microsoft. 2012. Best Practices Analyzer for Active Directory Domain Services. Viitattu 26.7.2014. https://technet.microsoft.com/en-us/library/dd391875%28v=ws.10%29.aspx

Microsoft. 2012a. Configure Print and Document Services. Viitattu 4.1.2015. https://technet.microsoft.com/en-us/library/jj134163.aspx

Microsoft 2013. Active Directory Domain Services Overview. Viitattu 22.8.2014. https://technet.microsoft.com/en-us/library/hh831484.aspx

Microsoft. 2013a. Best Practices for Securing Active Directory. Viitattu 3.12.2014. https://technet.microsoft.com/en-us/library/dn487446.aspx

Microsoft. 2013b. Best Practices for Shadow Copies of Shared Folders. Viitattu 10.1.2015
https://technet.microsoft.com/en-us/library/cc753975.aspx

Microsoft. 2013c. Windows Deployment Services Getting Started Guide for Windows Server 2012. Viitattu 20.7.2014.
https://technet.microsoft.com/en-us/library/jj648426.aspx

Microsoft. 2014. Active Directory FSMO roles in Windows. Viitattu 22.8.2014
http://support2.microsoft.com/kb/197132

Microsoft. 2014a. Windows Server Update Services Overview. Viitattu 3.12.2014.
https://technet.microsoft.com/en-us/library/hh852345.aspx

Microsoft. 2014b. Print and Document Services Architecture. Viitattu 17.10.2014
https://technet.microsoft.com/en-us/library/jj134171.aspx

Microsoft. 2014c. Deploy Windows Server Update Services in Your Organization. Viitattu 28.9.2014.
https://technet.microsoft.com/en-us/library/hh852340.aspx

Microsoft. n.d.b. How DNS Works. Viitattu 22.8.2014.
https://technet.microsoft.com/en-us/library/dd197446%28v=ws.10%29.aspx

Microsoft Solution Accelerators. 2011. Infrastructure Planning and Design, Active Directory Domain Services version 2.2. Viitattu 22.8.2014.
https://technet.microsoft.com/library/cc196387.aspx

Patrick Regan. 2013. Administering Windows Server 2012. Hoboken: John Wiley & Sons Inc. Viitattu 11.12.2014.

Suomen Taloushallintoliitto. 2012. Tietotekniikka ja työvälineet. Viitattu 15.3.2015
https://taloushallintoliitto-fi.directo.fi/jasensivut/tal-laatu/tukiprosessi/tietotekniikka-ja-tyovalineet/#anchor-1064695

Taylor Gibb. 2011. How to Understand Those Confusing Windows 7 File/Share Permissions. Viitattu 20.2.2015.
http://www.howtogeek.com/72718/how-to-understand-those-confusing-windows-7-fileshare-permissions/

Wakaru Official Course Material. 2012. Version 3.2
ITIL Foundation Certificate Syllabus V5.2 25 July 2011.
Viitattu 20.12.2014

Wikipedia. 2014a. IEEE 802.3. Viitattu 22.1.2015.
http://fi.wikipedia.org/wiki/IEEE_802.3

Wikipedia. 2014b. Active Directory. Viitattu 22.8.2014
http://en.wikipedia.org/wiki/Active_Directory

Wikipedia. 2015a. Lähiverkko. Viitattu 22.1.2015.
http://fi.wikipedia.org/wiki/L%C3%A4hiverkko

Wikipedia. 2015b. Ethernet. Viitattu 22.1.2015.
http://fi.wikipedia.org/wiki/Ethernet

Wikipedia. 2015c. Verkkotopologia. Viitattu 22.1.2015.
http://fi.wikipedia.org/wiki/Verkkotopologia

Wikipedia. 2015d. Palomuuri. Viitattu 22.1.2015.
http://fi.wikipedia.org/wiki/Palomuuri

Wikipedia. 2015e. Reverse DNS Lookup. Viitattu 20.1.2015.
http://en.wikipedia.org/wiki/Reverse_DNS_lookup

Wikipedia. 2015f. File Server. Viitattu 15.1.2015.
http://en.wikipedia.org/wiki/File_server

Wikipedia. 2015g. ISO/IEC 27000-series. Viitattu 2.2.2015.
http://en.wikipedia.org/wiki/ISO/IEC_27000-series

Tilitoimiston toimistopäällikön kertomus alkutilanteesta

Yritys on auktorisoitu Taloushallintoliiton jäsenyritys. Taloushallintoliiton toimialastandardi on tarkoitettu taloushallinnon palveluyrityksille ja muille taloushallinnon asiantuntijapalveluita tarjoaville toimijoille avuksi alan hyvän tavan noudattamiseen. Toimialastandardi asettaa taloushallinnon palveluyrityksen toiminnalle laadullisen vaatimustason, jota noudattamalla taloushallinnon palveluyritys voi tuottaa laadukasta palvelua ja oikeaa tietoa asiakkaalle ja viranomaisille, sekä muille sidosryhmille. Taloushallinnon palvelut muuttuvat ja saavat uusia muotoja, esimerkiksi teknisten innovaatioiden, kehittyvän lainsäädännön ja markkinoihin sopeutumisen seurauksena. TAL-STA2–toimialastandardin 1.7 kohdan mukaisesti palvelujen lähtökohtana on luottamuksellisuus asiakkaan ja taloushallinnon palveluyrityksen välillä. Asiakkaan toimeksiantoon liittyvä aineisto, liikesalaisuudet ja muut luottamukselliset tiedot, sekä niiden perusteella taloushallinnon palveluyrityksen tuottama tieto, on turvattava. Tiedon turvaamisella tarkoitetaan standardissa teknisiä, fyysisiä ja henkilöiden toimia koskevia menettelyjä. Jatkuvasta asiakastiedostojen varmistuksesta tulee huolehtia ja tietosuojasta annettujen lakien vaatimukset ja suositukset on otettava huomioon. Toimeksiannoissa korostuu luottamuksellisuus mm. palkanlaskennan tietojen arkaluonteisuuden vuoksi. Mikäli viranomais- tai muu taho pyytää palkanlaskentatietoja, tulee varmistua vastaanottajan oikeudesta saada tietoja. Standardi suosittelee solmittavaksi kaikkien työ- tai sopimussuhteessa olevien kanssa kirjalliset salassapitosopimukset.
Taloushallintoliiton yleisten sopimusehtojen KL2004 mukaisesti yrityksen tulee vastata tietoturvallisuudesta ja huolehtia viruksentorjunta- ja muiden suojausjärjestelmien kunnosta ja ajanmukaisuudesta. Yrityksen tulee tietää ja hyväksyä, että sähköinen viestintä voi häiriytyä. Standardin mukaisesti sähköpostitse voidaan lähettää viestejä ja liitetiedostoja salaamattomina, jos muuta ei ole sovittu.
Taloushallintoliiton laatulomakkeisiin kuuluu lomake ”Itsearviointilomake tilitoimistossa käsiteltävien tietojen turvallisesta säilyttämisestä ja käsittelemisestä”. Yritys ei ole ottanut kantaa lomakkeen sisältöön.

Tietoturva

Palvelimen nauhavarmistuksen nauhat on säilytetty lukollisen, paloturvatun holvin sisällä olevassa lukollisessa kassakaapissa. Kassakaapin avain ja holvin avain ovat kätkettyinä yrityksen tiloissa ja niiden sijainnit ovat henkilöstön tiedossa. Asiakkailla ei ole pääsyä holviin, vaikka holvin ovi on päiväsaikaan kiinni mutta lukitsematta. Asiakkaiden materiaalit säilytetään työntekijöiden työhuoneissa. Työtilat ovat avoimia ja niihin ei ole lukittavia ovia. Asiakasmateriaaleissa (mapeissa) ei ole asiakkaan tunnistavia tekstejä näkyvissä. Työpöydät pyritään pitämään tyhjinä silloin, kun työntekijä ei ole paikalla.
Asiakkaan arkaluontoinen materiaali saattaa antaa toiselle asiakkaalle merkittävää tietoa. Yritys ei ole joutunut korvaamaan vääriin käsiin joutunutta tietoa, eikä tilanteita, jossa tietoa olisi vuotanut vääriin käsiin, ole tullut eteen.

Uhka, että paperilla säilytettävää aineistoa katoaisi tai joutuisi vääriin käsiin, on ollut yrityksen mielestä pieni. Yrityksessä ei ole tiloja, joista tietoa voisi huomaamatta kadota, henkilöstöllä on näkyvyys kaikkiin avoimiin tiloihin.

Varmistukset

Taloushallinnon ohjelmisto on SaaS-sovellus, ohjelmistotoimittaja varmistaa tietokannat päivittäin. Lisäksi käyttäjät ottavat varmistuksia tietokannoista asiakaskohtaisesti päivittäisistä tilanteista ja nämä varmistukset ovat mukana ohjelmistotoimittajan varmistusten tallenteessa.

Yrityksellä on kaksi palvelinta, joille tallennetaan kaikki word- ja excel-ohjelmilla tehdyt tiedostot, sähköpostien pst-tiedostot ja kaikki muu materiaali (ei talousohjelmiston tietokantaa). Yrityksellä on käytössä kaksi ohjelmaa, jotka on tallennettu omalle palvelimelle ja joiden tietokannat ovat serverillä. Henkilöstölle on ohjeistettu, että mitään tiedostoja ei saa olla tallennettuna omilla työasemilla, koska niistä ei oteta varmistuksia. Servereillä olevat tiedot on varmistettu ajastetusti päivittäin nauhavarmistuksella. Ennen nauhavarmistusta toisen serverin tiedot (jotka ulkopuolinen toimittaja on jossakin vaiheessa määritellyt tärkeiksi varmistettaviksi tiedoiksi) on kopioitu serverille, jolla on nauha-asema. Nauhavarmistus on kestänyt koko yön ja ei ole aina ollut valmiina aamulla ennen työpäivän alkua.

Syksyllä 2013 havaittiin, että serverien välinen tietojen kopiointi ei ole toiminut ilmeisesti pitkään aikaan. Ongelma tuli esille, kun haluttiin palauttaa varmistuksesta tietoa, joka oli kadonnut. Varmistus ei siis ollut toiminut halutulla tavalla.

Käyttäjätilit

Käyttäjätilejä ei ole varsinaisesti hallinnoitu. Käyttäjillä on kiinteät salasanat, eikä niitä ole vaihdettu. Servereitä on kaksi ja kummallakin on sama salasana. Serverien salasana on tiedossa koko henkilöstöllä. Käyttäjien salasanat on muodostettu siten, että henkilöstö voi halutessaan käyttää toistensa käyttäjätunnuksia. Yrityksessä käy tilintarkastajia, joille on luotu yhteinen käyttäjätunnus järjestelmiin. Käyttäjätunnusten ja salasanojen käytäntö on ollut yrityksessä käytössä yli 10 vuotta ja järjestelmään sisältyvää riskiä ei ole aikaisemmin tiedostettu.

Liite 2

Yrityksen tavoitteet

Sovitaan yrityksen laitteisto- ja ohjelmistomuutoksen toteuttaminen mahdollisimman pikaisesti. Pyydetään muutoksen toteuttajaksi ammattitaitoinen osaaja.
Yritykselle hankitaan uusi serveri. Serverin tietoturva luodaan mahdollisimman hyväksi ja hankitaan serverille uusi nauhavarmistusasema. Käyttäjätunnus- ja salasanakäytäntö muutetaan vastaamaan tietoturvavaatimuksia. Tietoturvan parantamiseksi käyttäjien salasanat ovat vaihtuvia ja käyttäjien toimialuetta rajoitetaan vastaamaan käyttötarkoitusta.

Hankitaan vanhojen työasemien tilalle uudet työasemat. Työasemille asennetaan yhtenäinen käyttöjärjestelmä.
Työasemille hankitaan ja asennetaan yhtenäinen työkaluohjelmisto.
Hankitaan uusi palomuuri.

Tiedotetaan henkilöstölle tulevista muutoksista. Varmistutaan siitä, että henkilöstöllä on tarvittava osaaminen tietoturvallisuuden ylläpitämiseksi ja että asiakkaiden tietoa käsitellään huolellisesti ja säilytetään turvallisesti.

Yrityksen tietoturva- ja tietotekniikka-asioista vastaava henkilö perehdytetään uusiin käytäntöihin.
Taloushallintoliiton laatulomakkeisiin kuuluva lomake ”Itsearviointilomake tilitoimistossa käsiteltävien tietojen turvallisesta säilyttämisestä ja käsittelemisestä” käsitellään ja mahdollisiin ilmeneviin puutteisiin puututaan välittömästi. Tietoliikenteen sujuvuuden parantamiseksi sovitaan nopeampi yhteys.

Alkuperäiset allekirjoitetut dokumentit ovat asiakkaalle tärkeitä ja niitä tulee säilyttää huolella. Pyritään siirtämään kaikki alkuperäinen korvaamaton materiaali holviin tai luovuttamaan aineisto asiakkaan arkistoitavaksi.

Best Practices Checklist

Management Plane Checks

Disable Console Logging - Firewall		
Requirement	**Severity**	**Comments**
Disable Console Logging	Low	**Best practice:** Ensure console logging is disabled or set to critical. Although useful for troubleshooting from the console port, it is possible that excessive log messages on the console could make it impossible to manage the device, even from the console. **Command:** *no logging console* - *or* - *logging console critical*

Enable Logging - Firewall		
Requirement	**Severity**	**Comments**
Enable Logging	Info	**Best practice:** Check if state of event logging on the firewall is enabled. Logging a firewall's activities and status offers several benefits. Using the information in a log, the administrator can tell whether the firewall is working properly or whether it has been compromised. In some cases, it can show what types of probes or attacks are being attempted against the firewall or the protected network. If the logging is disabled, the events that happen on the firewall are not logged anywhere. This may make it harder to troubleshoot any network issues. This may also cause some of the problems, including attempted attacks, to go unnoticed, as well as prevent collection of evidence about any unauthorized activity. If logging is enabled, ensure the logging messages are sent to only trusted hosts on a protected network so the logs cannot be compromised and cannot be viewed by anyone who is not authorized to view them. **Command:** *logging on* | *logging enable*
Enable Logging Timestamp	Low	**Best practice:** Timestamps should be enabled for log messages, which will facilitate interpretation of the messages for troubleshooting and investigating network attacks. Ensure that the date/time is correctly set (if NTP is not configured) so that the timestamps provide the proper day/time of the log messages. If the timestamps are not shown in the log messages, it may not be possible to sense the order of events occurring in the network. **Command:** logging timestamp *logging timestamp*

Enable Logging to Buffer	Low	**Best practice:** Cisco devices can store log messages in memory. The buffered data is available only from an exec or enabled exec session, and it is cleared when the device reboots. This form of logging is useful, even though it does not offer enough long-term protection for the logs. Buffered logging keeps the log messages in RAM on the device. A logging buffer must be configured on the device, and this buffer is circular, meaning that when it fills up, the oldest log message is deleted to make room for the new message. If buffer logging is not enabled, it will not be possible to view the most recent log messages on the device for troubleshooting or monitoring purposes. **Command:** *logging buffered <level>*
Log Messages to a Syslog Server	Info	**Best practice:** Cisco devices can be configured to forward log messages to an external Syslog service. It is highly recommended that networks implement a logging structure based on a Syslog infrastructure. Proactive monitoring of firewall logs is an integral part of Security Admin duties. The firewall syslogs are useful for forensics, network troubleshooting, security evaluation, worm and virus attack mitigation, and so on. This is a scalable solution, which provides long-term storage capabilities and a central location for all device messages **Command:** *logging host <interface-name> <ipAddress>*

Secure Device Access - Firewall		
Requirement	**Severity**	**Comments**
Restrict HTTP Access to Certain Addresses	Info	**Best practice:** To specify hosts that can access the HTTP server internal to the FWSM. The addresses allowed to access the firewall using HTTP can be restricted. Any undefined IP address will not see the prompt at all. **Command:** *http <ip-address> <net-mask> <interface name>*
Restrict SSH Access to Certain Addresses	Medium	**Best practice:** The addresses allowed to access the firewall using SSH can be restricted. Any undefined IP address will not see the prompt at all. **Command:** *ssh <ip-address> <net-mask> <interface name>*
Restrict Telnet Access to Certain Addresses	Medium	**Best practice:** The addresses allowed to access the firewall using Telnet can be restricted. Any undefined IP address will not see the prompt at all. **Command:** *telnet <ip-address> <net-mask> <interface name>*

Set Enable Password	Info	**Best practice:** Set enable password to secure access to privilege level. Access to the privileged EXEC mode (enable mode) should be protected by requiring a password else user logged in to user mode can access enable mode. **Command:** *enable password <password>*
Set Password	Info	**Best practice:** To set the login password, use the **passwd** command in global configuration mode. You are prompted for the login password when you access the CLI as the default user using Telnet or SSH. After you enter the login password, you are in user EXEC mode. **Command:** *passwd <password>*
Set Suitable Console Timeout	Low	**Best practice:** For console connections the idle timeout must be configured to avoid undesirable open and unattended console connection to the firewall. **Command:** *console timeout <timeout value in minutes>*
Set Suitable SSH Timeout	Low	**Best practice:** For ssh connections the idle timeout must be configured to avoid undesirable and unattended open ssh connections to the firewall. **Command:** *ssh timeout <timeout in minutes>*
Set Suitable Telnet Timeout	Low	**Best practice:** For telnet connections the idle timeout must be configured to avoid undesirable open unattended telnet connection to the firewall. **Command:** *telnet timeout <timeout in minutes>*
Use Warning Banner Messages	Low	**Best practice:** Use of configurable, personalized login and failed-login banners is recommended. This feature lets you change the default message for login and failed-login. You can configure message banners that will be displayed when a user logs in to the system **Command:** *banner <banner-message>*

Secure Interactive Access Using AAA - Firewall		
Requirement	**Severity**	**Comments**
Define AAA Server with Key	Medium	**Best practice:** An Authentication Authorization and Accounting Server (AAA) is recommended to store all the username / password and privilege levels in one single repository. AAA server should be configured with a key for authentication and encryption. **Command:** *aaa-server TACACS+ <interface> host <ipAddress> <key>*

Use AAA Accounting	Low	**Best practice:** When you configure the aaa accounting command, each command other than show commands entered by an administrator is recorded and sent to the accounting server or servers. **Command:** *aaa accounting command EXAUTH LOCAL*
Use AAA Authentication for Enable Mode	Medium	**Best practice:** Authenticates users who access privileged EXEC mode when they use the enable command. For authentication an external server may be used and also supports fallback to local database if external authentication server is down. **Command:** *aaa authentication enable console RADIUS LOCAL*
Use AAA Authentication for HTTP	Medium	**Best practice:** If aaa authentication http console command is not defined, you can gain access to the FWSM (via ASDM) with no username and the FWSM enable password (set with the enable password command). **Command:** *aaa authentication http console RADIUS LOCAL*
Use AAA Authentication for SSH	Info	**Best practice:** Before the firewall can authenticate a Telnet or SSH user, we must first configure access to the firewall using the telnet or ssh commands. These commands identify the IP addresses that are allowed to communicate with the firewall. **Command:** *aaa authentication ssh console RADIUS LOCAL*
Use AAA Authentication for Telnet	Medium	**Best practice:** Before the firewall can authenticate a Telnet or SSH user, we must first configure access to the firewall using the telnet or ssh commands. These commands identify the IP addresses that are allowed to communicate with the firewall. **Command:** *aaa authentication telnet console RADIUS LOCAL*

Use AAA Authorization	Low	**Best practice:** The aaa authorization command specifies whether command execution at the CLI is subject to authorization. If you enable TACACS+ command authorization, and a user enters a command at the CLI, the FWSM sends the command and username to the TACACS+ server to determine if the command is authorized. When configuring command authorization with a TACACS+ server, do not save your configuration until you are sure it works the way you want. If you get locked out because of a mistake, you can usually recover access by restarting the FWSM. **Command:** *aaa authorization command TACACS LOCAL*
Use Local Login as Backup to AAA	Info	**Best practice:** While configuring external authentication it is advisable to keep the local database check as fallback option. **Command:** *aaa authentication http console RADIUS LOCAL*

Secure Management Protocols - Firewall		
Requirement	**Severity**	**Comments**
Authenticate NTP Updates	Medium	**Best practice:** Network Time Protocol (NTP) is a UDP based protocol used to synchronize time clocks amongst network devices. NTP is especially useful to ensure that timestamps on log messages are consistent throughout the entire network. It is recommended to authenticate NTP updates so that time is synchronized with approved servers only. **Command:** *ntp authentication-key <key-id> md5 <key>*
Change Default Community String	High	**Best practice:** The default community string of "public" and "private" are well known. These should always be changed to more secure strings. **Command:** *snmp-server community <non-default-string>*
Define SNMP Server Host	Low	**Best practice:** SNMP is an application-layer communication protocol that allows ONS 15454 network devices to exchange management information among these systems and with other devices outside the network. SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. **Command:** *snmp-server host*

Disable SNMP if not used	Low	**Best practice:** SNMP Protocol should be disabled if not used in the network. If used, access to SNMP service should be protected using appropriate mechanisms like ACLs. **Command:** *no snmp-server*
Enable SNMP Trap Logging	Low	**Best practice:** SNMP traps are used to report an alert or other asynchronous event about a managed firewall. **Command:** *snmp server enable traps*
Use NTP to Synch Network Clocks	Medium	**Best practice:** Network Time Protocol (NTP) is a UDP based protocol used to synchronize time clocks amongst network devices. NTP is especially useful to ensure that timestamps on log messages are consistent throughout the entire network. **Command:** *ntp server <ntp server name> source <interface>*

Control Plane Checks

Disable Unneeded Services - Firewall		
Requirement	**Severity**	**Comments**
Check if Failover is used	Info	**Best practice:** This rule checks if failover is configured in the firewall devices **Command:** *failover*
Disable HTTP session replication	Info	**Best practice:** The replication of http session data to the failover firewall should be disabled unless the firewall is not expected to be under extreme load and the http session data is highly critical. Given the short duration of http sessions, low probably of firewall failure and the design of most applications, this is not likely to be needed. This rule checks only firewalls with failover configured. **Command:** *no failover replication http*

Disable Proxy ARPs	Low	**Best practice:** Proxy ARP allows a firewall to extend the network at layer 2 across multiple interfaces (i.e. LAN segments). Hence proxy ARP allows hosts from different segments to function as if they were on the same subnet, and is only safe when used between trusted LAN segments. Attackers can use the trusting nature of proxy ARP by spoofing a trusted host and intercepting packets. Because of this inherent security weakness, proxy ARP should be disabled on interfaces that do not require it, especially those interfaces that connect to untrusted networks. **Command:** *sysopt noproxyarp <interface>*
Limit ICMP responses on interfaces	Low	**Best practice:** Preferable to disable ICMP on outside interfaces at a minimum. The default (i.e. no ICMP control list is configured), is for the PIX/ASA/FWSM to accept all ICMP traffic that terminates at any interface (including the outside interface). This will depend on the customer policy. **Command:** *icmp permit <acl> <interface>*

Data Plane Checks

There are numerous techniques of securing the data plane in firewalls, which will be discussed in this section. Packet filtering, stateful inspection, proxies and application level inspection are one of the basic aspects of data plane security.

It is never recommended to rely on one method of data plane security alone. It is best to use a combination of methods available as covered in this section.

Data Plane - Firewall		
Requirement	**Severity**	**Comments**
Enable uRPF anti-spoofing	Info	**Best practice:** Anti-spoofing should be configured on all outside interfaces. This rule checks if uRFP is enabled on any one interface. **Command:** *ip verify reverse-path interface <interface-name>*

AD DS Best Practices

Prerequisites:
AD DS: The domain controller must be able to connect to the RID master in this domain
AD DS: The domain controller must be able to connect to the PDC emulator master in this domain
AD DS: This domain controller must be able to reach a DNS server and retrieve DNS records that are associated with this domain controller

Configuration:
AD DS: The RID master role and the PDC emulator master role should be owned by the same domain controller in the domain
AD DS: This domain controller must register its DNS host A/AAAA records with correct IP addresses
AD DS: This domain controller must register its DNS host A/AAAA records
AD DS: This domain controller must register an alias (CNAME) resource record with its DsaGuid for the forest
AD DS: This domain controller must register its Rfc1510UdpKpwd DNS record to advertise itself as a Kerberos server for the domain
AD DS: This domain controller must register its Rfc1510Kpwd DNS record to advertise itself as a Kerberos server for the domain
AD DS: This domain controller must register its Rfc1510UdpKdc DNS record to advertise itself as a Kerberos server for the domain
AD DS: This domain controller must advertise itself as a generic global catalog server for the forest in its local site
AD DS: This domain controller must advertise itself as a generic global catalog server for the forest
AD DS: This domain controller must advertise itself as a Kerberos server for the domain in its local site
AD DS: This domain controller must register its Rfc1510Kdc DNS record to advertise itself as a Kerberos server for the domain
AD DS: This server must advertise itself as a domain controller for the domain in its local site
AD DS: This server must advertise itself as a domain controller for the domain
AD DS: This domain controller must advertise as a KDC for the domain in its local site
AD DS: This domain controller must advertise as a KDC for the domain
AD DS: This global catalog server must register its host (A/AAAA) resource records for the forest
AD DS: This domain controller must register a DNS SRV resource record, which is required for replication to function correctly
AD DS: This domain controller must advertise as a global catalog server for the forest in its local site
AD DS: This domain controller must advertise as the global catalog server for the forest
AD DS: This domain controller must advertise as a PDC for the domain

AD DS: This domain controller must advertise as an LDAP server for the domain in its local site
AD DS: This domain controller must advertise as an LDAP server for the domain
AD DS: This domain controller must register its DNS host (A/AAAA) resource records for the domain
AD DS: The schema master role and the domain naming master role should be owned by the same domain controller in the forest
AD DS: The AD DS service must be running on this domain controller
AD DS: The ADWS service must be running on this domain controller
AD DS: The Active Directory module for Windows PowerShell must be installed and functioning properly on this domain controller
AD DS: The AD DS BPA should be able to collect data for this element
AD DS: Strict replication consistency should be enabled on all domain controllers in this forest
AD DS: Each site in this forest should contain at least one global catalog server or have universal group membership caching enabled
AD DS: The KCC should be enabled in this site in this forest to generate an optimal replication topology
AD DS: The value of MaxPosPhaseCorrection on this domain controller should be equal to 48 hours
AD DS: The value of MaxNegPhaseCorrection on this domain controller should be equal to 48 hours
AD DS: The PDC emulator master in this forest should be configured to correctly synchronize time from a valid time source
AD DS: This domain controller should comply with the recommended best practices guidelines because it is running on a VM
AD DS: This directory partition on this domain controller should have been backed up within the last 8 days
AD DS: All Ous in this domain should be protected from accidental deletion
AD DS: The resultant backup lifetime in this forest should be equal to or greater than 180 days
AD DS: SID filtering is not enabled for an external trust
AD DS: An account or accounts trust(s) this unregistered SPN for delegation
AD DS: This Service Principal Name is registered on multiple accounts
AD DS: User accounts and trusts in this domain should not be configured for DES only
AD DS: This domain controller must have “Access this Computer from the Network” granted to the appropriate security principals
AD DS: This domain controller must have “Enable computer and user accounts to be trusted for delegation“ granted to the Builtin Administrators security group
AD DS: The infrastructure master for this domain should be held by a domain controller that is not a global catalog server
AD DS: The Default Domain Controllers Policy in this domain should be applied to this OU

Operation:
AD DS: All domains should have at least two functioning domain controllers for redundancy

DNS Best Pratices

Configuration:
DNS: DNS servers on <adapter name> should include their own IP addresses on their interface lists of DNS servers
DNS: IP addresses that belong to a valid range must be configured on <adapter name>
DNS: <Adapter name> must have configured DNS servers
DNS: Network interfaces on <adapter name> must be configured with DNS servers that belong to a valid IP address range
DNS: <Adapter name> should be configured to use both a preferred and an alternate DNS server
DNS: <Adapter name> should have static Ipv4 settings
DNS: IP addresses must be configured on <adapter name>
DNS: Valid network interfaces should precede invalid interfaces in the binding order
DNS: DNS servers on <adapter name> should include the loopback address, but not as the first entry
DNS: If the Global Query Block List is enabled, then it should not be empty
DNS: Cache locking should be configured to 90% or greater
DNS: The forwarding timeout value should be 2 to 10 seconds
DNS: The Hosts file <file name> on the DNS server should be empty
DNS: Interface <adapter name> on the DNS server should be configured to register its IP addresses in DNS
DNS: The DNS server must have root hints or forwarders configured
DNS: The scavenging interval <interval value> is within the recommended range
DNS: The DNS server should have scavenging enabled
DNS: The scavenging interval <interval value> is not set to a recommended value
DNS: Zone <zone name> has scavenging enabled with recommended parameters
DNS: Zone <zone name> has record aging disabled, so scavenging will not occur
DNS: Zone <zone name> scavenging server list should not be empty
DNS: Zone <zone name> scavenging parameters should be set to default values
DNS: The socket pool should be enabled with recommended settings
DNS: The recursion timeout must be greater than the forwarding timeout
DNS: Forwarding server <IP address> should respond to DNS queries
DNS: At least one DNS server on the list of forwarders must respond to DNS queries
DNS: The list of forwarding servers must not contain the link-local IP address <IP address>
DNS: The list of forwarding servers must not contain the loopback address <IP address>
DNS: More than one forwarding server should be configured

DNS: Zone <zone name> master server list must not be empty
DNS: Zone <zone name> update notification list must not be empty
DNS: Zone <zone name> secondary servers list should not be empty
DNS: Zone <zone name> should be present on the secondary server <IP address> configured to receive zone update notifications
DNS: Zone <zone name> scavenging servers should host the zone
DNS: The list of root hints must not contain the link-local IP address <IP address>
DNS: The list of root hints must not contain the host IP address or loop-back address <IP address>
DNS: The list of root hints should contain more than one entry
DNS: Zone <zone name> is Active Directory integrated and should be present and configured as primary
DNS: Zone <zone name> is an Active Directory integrated DNS Zone and must be available
DNS: Zone <zone name> is an Active Directory integrated DNS zone and must be configured as primary
DNS: Zone <zone name> transfers from the primary to the secondary DNS server must be successful

Operation:
DNS: The DNS server <IP address> on <adapter name> must be able to resolve names in the forest root domain name zone
DNS: The DNS server <IP address> on <adapter name> must be able to resolve names in the primary DNS domain zone
DNS: The DNS server <IP address> on <adapter name> must resolve Global Catalog resource records for the domain controller
DNS: The DNS server <IP address> on <adapter name> must resolve Kerberos resource records for the domain controller
DNS: The DNS server <IP address> on <adapter name> must resolve LDAP resource records for the domain controller
DNS: The DNS server <IP address> on <adapter name> must resolve PDC RRs for the domain controller
DNS: The DNS server <IP address> on <adapter name> must resolve the name of this computer
DNS: DNS servers assigned to the network adapter should respond consistently
DNS: Zone <zone name> master servers must respond to queries for the zone
DNS: Zone <zone name> secondary servers must respond to queries for the zone
DNS: Zone <zone name> master server <IP address> must respond to queries for the zone
DNS: Zone <zone name> secondary server <IP address> should respond to queries for the zone
DNS: Root hint server <IP address> must respond to NS queries for the root zone
DNS: At least one name server in the list of root hints must respond to queries for the root zone

DNS: The DNS server configured on the adapter <adapter name> should resolve the name of this computer
DNS: Zone <zone name> is an Active Directory integrated DNS zone and must be running

File Services Best Practices

Configuration:
DFS-N: The DFS Namespace service startup type should be set to Automatic
DFS-N: All IP addresses for the server should map to the same AD DS site
DFS-N: The LDAP timeout value should be set to the default value of 30 seconds
DFS-N: The DFS Namespaces sync interval should be set to the default value of 1 hour
DFS-N: Site costed referrals should be enabled on domain controllers
DFS-N: Client failback should be enabled for the Netlogon and SYSVOL folders on domain controllers
DFS-N: Namespace root referrals should use the Lowest Cost ordering method on the following DFS namespace
DFS-N: Failover Clustering should be enabled on the server hosting the following standalone namespace
DFS-N: Additional namespace servers should be added to the following domain-based namespace
DFS-N: Windows Server 2008 mode can be used on the following domain-based namespace
DFS-N: The access-based enumeration setting should be identical in the DFS namespace database and on the shared folder hosting the namespace root for the following namespace
DFS-N: Client failback should be enabled on the following namespace
DFS-N: The namespace server should be enabled on the following namespace
DFS-R: The DFS Replication service should be started and have a startup type set to Automatic
DFS-R: Replicated folder must be enabled for replication
DFS-R: Servers ‘{0}’ and ‘{1}’ belonging to the replication group ‘{2}’ must have two-way connections between them
FSRM: File Server Resource Manager should be installed on all nodes of a failover cluster
FSRM: The shadow copy storage area should be large enough for File Server Resource Manager to create snapshots of files
FSRM: Classified files should have read/write attributes
FSRM: File paths should be shorter than 240 characters
FSRM: Alternate data streams should be large enough to store classification properties
FSRM: The cache for classification properties should be active
FSRM: There should be fewer than 1000 file screens configured on the server
FSRM: There should be fewer than 1000 quotas configured on the server
FSRM: There should be fewer than 20 classification properties
FSRM: Classification rules should have schedules
FSRM: Notifications that use variables that reference remote paths should reference valid shared folders

NFS: The domain functional level should be Windows Server 2003 R2 or higher when using an identity mapping solution
NFS: Folders that are shared by using both the SMB and NFS protocols should use mapped accounts
NFS: Server for NFS should be configured to use Netgroups
NFS: Services for Network File System should use an RFC 2307-based identity mapping solution
NFS: Operating system case sensitivity should be disabled for file servers that support the NFS and SMB protocols
NFS: Windows Firewall should open all ports used by Services for Network File System
NFS: Services for Network File System should be used or uninstalled
NFS: The Server for NFS service should be started
SMB: The Server service should be set to start automatically
SMB: File and printer sharing ports should be open
SMB: Previous Versions support for client computers running Windows 98 should be disabled
SMB: The SMB 2.0 file sharing protocol should be enabled

Operation:
DFS-N: The DFS Namespace service should be started
DFS-R: The read-only mini-filter driver must always be loaded on servers that have read-only DFS replicated folders
DFS-R: The DFS Replication service needs sufficient disk space to store replication conflicts for the replicated folder
DFS-R: There should not be a large number of replication conflicts in the replicated folder '{0}'
DFS-R: Volumes hosting replicated folders should have sufficient free disk space
DFS-R: The staging folder for the replicated folder should not require frequent cleanup
FSRM: Log files for file management tasks should be properly deleted
FSRM: All nodes in a failover cluster should be reachable
FSRM: The File Server Resource Manager service should be running

Performance:
FSRM: The File Server Storage Reports Manager service should stop when not in use
SMB: Short file name creation should be disabled
SMB: No registry setting for tuning the number of TCP table partitions in TCP/IP should exist
SMB: No registry setting for tuning the TCP window size in TCP/IP should exist
SMB: No registry setting for tuning the MaxHashTableSize in TCP/IP should exist

Security:
NFS: Anonymous access should be disabled
SMB: Denial of service detection should be enabled

SMB: Digitally signed communication should be required or disabled

Liite 7

Windows Server Update Services Best Practices

Prerequisites:
WSUS: The Windows Server Update Services Role should be installed

Configuration:
WSUS: WSUS should be installed on a non-domain controller

Operation:
WSUS: The SelfUpdate folder should be installed correctly on the default Web site or the WSUS Administration site

Performance:
WSUS: Only required languages should be selected in the WSUS Configuration Wizard
WSUS: WSUS content should be installed on a nonsystem drive
WSUS: WSUS database should be installed on a nonsystem drive

PIX501 konfiguraatio

```
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password l7sFQPU8HeQqS8fK encrypted
passwd l7sFQPU8HeQqS8fK encrypted
hostname markkumakelapix501
domain-name markkumakela.fi
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside xxx.xxx.xxx.xxx 255.255.255.248
ip address inside 192.168.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm logging informational 100
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 yyy.yyy.yyy.yyy 1
timeout xlate 0:05:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225
1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa authentication ssh console LOCAL
aaa authentication telnet console LOCAL
aaa authentication enable console LOCAL
```

```
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 5
ssh zzz.zzz.zzz.zzz 255.255.255.255 outside
ssh www.www.www.www 255.255.255.255 outside
ssh 192.168.1.0 255.255.255.0 inside
ssh timeout 15
console timeout 0
dhcpd address 192.168.1.10-192.168.1.129 inside
dhcpd dns 192.168.1.5
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd domain makela.local
dhcpd enable inside
username tcadmin password 3udm.vPlEVdKlGTU encrypted privilege 15
username makela password l7sFQPU8HeQqS8fK encrypted privilege 15
terminal width 80
Cryptochecksum:6e570ec94b434168f5845bb9845bb78e
: end
```

Liite 9

Tarjouspyyntö laitteista

TARJOUSPYYNTÖ 24.2.2014

PALVELIN, TYÖASEMAT JA KÄYTTÖJÄRJESTELMÄT

Pyydän tarjoustanne 7.3.2014 mennessä yrityksemme uudesta palvelimesta, työasemista ja käyttöjärjestelmistä seuraavasti

Uudet laitteet ja niille käyttöjärjestelmät

Palvelin 1 kpl
- RAM minimi 8gb mielellään 16gb
- Intel Xeon prosessori
- 4x500gb raid10 (hot swap)
- nauhavarmistin
- kirjoittava dvd- asema
- windows server 2012 R2 standard 64-bit

Työasemat 5 kpl
- windows 7 pro sp1 64-bit
- 4gb ram
- 4-ydin prosessori
- 500gb kovalevy
- kirjoittava dvd- asema

Toimitus 11.4.2014 mennessä.

Liite 10

Tarjous laitteista

Palvelinrautaratkaisu:
Fujitsu PRIMERGY TX-200 palvelin
16 Gt keskusmuistia
1 x Xeon E5-2407 prosessori
1 x Raid-ohjain
2 x verkkokortti
1 x virtalähde
4 x 500 Gt SATA kovalevyä (raid 10)
DVD +- RW
kolmen vuoden takuu, onsite- vasteaika seuraavan työpäivän aikana
1 x WIN 2012 Server R2 Standard palvelinohjelmisto
Symantec Backup Exec 2012 varmuuskopiointiohjelmisto
LTO4 varmistusasema + 5 kpl varmistusnauhoja
Rauta kasattuna ja testattuna sekä käyttöjärjestelmä asennettuna

Työasemat
5 x Fujitsu Esprimo P420 työasema
Intel Core i5 prosessori
4 Gt keskusmuisti
500 Gt kovalevy
Win 7 Professional käyttöjärjestelmä, 64 bit / Win 8.1 Pro lisenssi
DVD +- RW
3 vuoden Onsite takuu, vasteaika seuraavan työpäivän aikana
Office 2013 (word, excel, powerpoint ja outlook)

Lisäksi 20kpl Windows Server 2012 R2 standard User CAL

Google/Google Update/Applications
Policy Setting Comment
Update policy override default Enabled
Policy Always allow updates (recommended)

Google/Google Update/Applications/Google Chrome
Policy Setting Comment
Allow installation Enabled
Update policy override Enabled
Policy Always allow updates (recommended)

Google/Google Update/Applications/Google Chrome Binaries
Policy Setting Comment
Allow installation Enabled
Update policy override Enabled
Policy Always allow updates (recommended)

Google/Google Update/Preferences
Policy Setting Comment
Auto-update check period override Enabled
Minutes between update checks 1400
Disable all auto-update checks (not recommended) Disabled

Network/Network Connections/Windows Firewall/Domain Profile
Windows Firewall: Allow ICMP exceptions Enabled
Allow outbound destination unreachable Disabled
Allow outbound source quench Disabled
Allow redirect Disabled
Allow inbound echo request Enabled
Allow inbound router request Disabled
Allow outbound time exceeded Disabled
Allow outbound parameter problem Disabled
Allow inbound timestamp request Disabled
Allow inbound mask request Disabled
Allow outbound packet too big Disabled

Windows Firewall: Allow inbound file and printer sharing exception Enabled
Allow unsolicited incoming messages from these IP addresses: 192.168.1.0/24

Windows Firewall: Allow inbound remote administration exception Enabled
Allow unsolicited incoming messages from these IP addresses: 192.168.10/24

Windows Firewall: Allow inbound Remote Desktop exceptions Enabled
Allow unsolicited incoming messages from these IP addresses: 192.168.1.0/24

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Connection
Allow users to connect remotely by using Remote Desktop Services Enabled

Mozilla Firefox/Addins and Updates
Allow Update and Auto Update Firefox Enabled
Allow Update and Auto Update Firefox Extensions Enabled
Suppress Firefox Updated Page After Update Enabled

Windows Components/Windows Installer
Always install with elevated privileges Enabled

System/Logon
Always wait for the network at computer startup and logon Enabled

Control Panel/Programs
Hide "Programs and Features" page Enabled

Interactive Logon
Interactive logon: Do not display last user name Enabled

Control Panel/Printers
Point and Print Restrictions Disabled

Network/DNS Client
Register DNS records with connection-specific DNS suffix Enabled
Register PTR records Enabled
Register PTR records: Register only if A record registration succeeds

Folder options
General
Properties
Always show icons, never thumbnails Disabled
Always show menus Disabled
Display file icon on thumbnails Enabled
Display file size information in folder tips Enabled
Display simple folder view in Navigation pane Enabled
Display the full path in the titlebar (classic folders only) Disabled
Hidden files and folders Do not show hidden files and folders
Hide extensions for known file types Disabled
Hide protected operating system files (Recommended) Enabled
Launch folder windows in separate process Disabled
Remember each folder's view settings Enabled
Restore previous folder windows at logon Disabled

Show drive letters Enabled
Show encrypted or compressed NTFS files in color Enabled
Show pop-up description for folder and desktop items Enabled
Show preview handlers in preview pane Enabled
Use check boxes to select items Disabled
Use sharing wizard (Recommended) Enabled
When typing into list view Select the typed item in the view
Common
Options
Stop processing items on this extension if an error occurs on this item No
Run in logged-on user's security context (user policy option) Yes
Apply once and do not reapply No

Power Options
Properties
Action Update
Make this the active Power Plan: Enabled
Name High performance
When computer is: Plugged in Running on batteries
Require a password on wakeup: Yes Yes
Turn off hard disk after: Never Never
Sleep after: Never Never
Allow hybrid sleep: Off Off
Hibernate after: Never Never
Lid close action: Sleep Sleep
Power button action: Shutdown Shutdown
Start menu power button: Hibernate Hibernate
Link State Power Management: Off Off
Minimum processor state: After 100 minutes After 5 minutes
Maximum processor state: After 100 minutes After 100 minutes
Turn off display after: After 15 minutes After 10 minutes
Adaptive display: On On
Critical battery action: Do nothing Shutdown
Low battery level: After 10 minutes After 10 minutes
Critical battery level: After 5 minutes After 5 minutes
Low battery notification: Off Off
Low battery action: Do nothing Do nothing

Common
Stop processing items on this extension if an error occurs on this item No
Remove this item when it is no longer applied No
Apply once and do not reapply No
Item-level targeting: Security GroupAttribute Value
bool AND
not 0
name TTMAKELA\GG_Makela_WKS
sid S-1-5-21-3677548916-3608000974-4182778928-1150
userContext 0
primaryGroup 0

localGroup 0

Windows Components/Windows Updatehide
Configure Automatic Updates Enabled
Configure automatic updating: 3 - Auto download and notify for install
The following settings are only required and applicable if 4 is selected.
Install during automatic maintenance Disabled
Scheduled install day: 0 - Every day
Scheduled install time: 11:00

Policy Setting Comment
Enable client-side targeting Enabled
Target group name for this computer Makela Desktop

Policy Setting Comment
Specify intranet Microsoft update service location Enabled
Set the intranet update service for detecting updates: http://MTSrv01.TTMAKELA.LOCAL:8530
Set the intranet statistics server: http://MTSrv01.TTMAKELA.LOCAL:8530

Local Policies/Security Optionshide
Devices
Policy Setting
Devices: Prevent users from installing printer drivers Disabled

Printers
Point and Print Restrictions Disabled

System/Driver Installation
Allow non-administrators to install drivers for these device setup classes Enabled
Allow Users to install device drivers for these classes:
{4d36e979-e325-11ce-bfc1-08002be10318}
{4658ee7e-f050-11d1-b6bd-00c04fa372a7}

Liite 12/1

Tietoturvasuunnitelman sisältö

4 RISK ASSESSMENT AND TREATMENT
4.1 ASSESSING SECURITY RISKS
4.2 TREATING SECURITY RISKS
5 SECURITY POLICY
5.1 INFORMATION SECURITY POLICY
5.1.1 Information security policy document
5.1.2 Review of the information security policy
6 ORGANIZATION OF INFORMATION SECURITY
6.1 INTERNAL ORGANIZATION
6.1.1 Management commitment to information security
6.1.2 Information security co-ordination
6.1.3 Allocation of information security responsibilities
6.1.4 Authorization process for information processing facilities
6.1.5 Confidentiality agreements
6.1.6 Contact with authorities
6.1.7 Contact with special interest groups
6.1.8 Independent review of information security
6.2 EXTERNAL PARTIES
6.2.1 Identification of risks related to external parties
6.2.2 Addressing security when dealing with customers
6.2.3 Addressing security in third party agreements
7 ASSET MANAGEMENT
7.1 RESPONSIBILITY FOR ASSETS
7.1.1 Inventory of assets
7.1.2 Ownership of assets
7.1.3 Acceptable use of assets
7.2 INFORMATION CLASSIFICATION
7.2.1 Classification guidelines
7.2.2 Information labeling and handling
8 HUMAN RESOURCES SECURITY
8.1 PRIOR TO EMPLOYMENT
8.1.1 Roles and resposiblities
8.1.2 Screening
8.1.3 Terms and conditions of employment
8.2 DURING EMPLOYMENT
8.2.1 Management responsibilities
8.2.2 Information security awareness, education, and training
8.2.3 Disciplinary process
8.3 TERMINATION OR CHANGE OF EMPLOYMENT
8.3.1 Termination responsibilities
8.3.2 Return of assets
8.3.3 Removal of access rights
9 PHYSICAL AND ENVIRONMENTAL SECURITY
9.1 SECURE AREAS
9.1.1 Physical security perimeter
9.1.2 Physical entry controls
9.1.3 Securing offices, rooms, and facilities
9.1.4 Protecting against external and environmental threats

9.1.5 Working in secure areas
9.1.6 Public access, delivery, and loading areas
9.2 EQUIPMENT SECURITY
9.2.1 Equipment siting and protection
9.2.2 Supporting utilities
9.2.3 Cabling security
9.2.4 Equipment maintenance
9.2.5 Security of equipment off-premises
9.2.6 Secure disposal or re-use of equipment
9.2.7 Removal of property
10 COMMUNICATIONS AND OPERATIONS MANAGEMENT
10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES
10.1.1 Documented operating procedures
10.1.2 Change management
10.1.3 Segregation of duties
10.1.4 Separation of development, test, and operational facilities
10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT
10.2.1 Service delivery
10.2.2 Monitoring and review of third party services
10.2.3 Managing changes to third party services
10.3 SYSTEM PLANNING AND ACCEPTANCE
10.3.1 Capacity management
10.3.2 System acceptance
10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE
10.4.1 Controls against malicious code
10.4.2 Controls against mobile code
10.5 BACK-UP
10.5.1 Information back-up
10.6 NETWORK SECURITY MANAGEMENT
10.6.1 Network controls
10.6.2 Security of network services
10.7 MEDIA HANDLING
10.7.1 Management of removable media
10.7.2 Disposal of media
10.7.3 Information handling procedures
10.7.4 Security of system documentation
10.8 EXCHANGE OF INFORMATION
10.8.1 Information exchange policies and procedures
10.8.2 Exchange agreements
10.8.3 Physical media in transit
10.8.4 Electronic messaging
10.8.5 Business information systems
10.9 ELECTRONIC COMMERCE SERVICES
10.9.1 Electronic commerce
10.9.2 On-Line Transactions
10.9.3 Publicly available information
10.10 MONITORING
10.10.1 Audit logging
10.10.2 Monitoring system use

10.10.3 Protection of log information
10.10.4 Administrator and operator logs
10.10.5 Fault logging
10.10.6 Clock synchronization
11 ACCESS CONTROL
11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL
11.1.1 Access control policy
11.2 USER ACCESS MANAGEMENT
11.2.1 User registration
11.2.2 Privilege management
11.2.3 User password management
11.2.4 Review of user access rights
11.3 USER RESPONSIBILITIES
11.3.1 Password use
11.3.2 Unattended user equipment
11.3.3 Clear desk and clear screen policy
11.4 NETWORK ACCESS CONTROL
11.4.1 Policy on use of network services
11.4.2 User authentication for external connections
11.4.3 Equipment identification in networks
11.4.4 Remote diagnostic and configuration port protection
11.4.5 Segregation in networks
11.4.6 Network connection control
11.4.7 Network routing control
11.5 OPERATING SYSTEM ACCESS CONTROL
11.5.1 Secure log-on procedures
11.5.2 User identification and authentication
11.5.3 Password management system
11.5.4 Use of system utilities
11.5.5 Session time-out
11.5.6 Limitation of connection time
11.6 APPLICATION AND INFORMATION ACCESS CONTROL
11.6.1 Information access restriction
11.6.2 Sensitive system isolation
11.7 MOBILE COMPUTING AND TELEWORKING
11.7.1 Mobile computing and communications
11.7.2 Teleworking
12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE
12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS
12.1.1 Security requirements analysis and specification
12.2 CORRECT PROCESSING IN APPLICATIONS
12.2.1 Input data validation
12.2.2 Control of internal processing
12.2.3 Message integrity
12.2.4 Output data validation
12.3 CRYPTOGRAPHIC CONTROLS
12.3.1 Policy on the use of cryptographic controls
12.3.2 Key management

12.4 SECURITY OF SYSTEM FILES
12.4.1 Control of operational software
12.4.2 Protection of system test data
12.4.3 Access control to program source code
12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES
12.5.1 Change control procedures
12.5.2 Technical review of applications after operating system changes
12.5.3 Restrictions on changes to software packages
12.5.4 Information leakage
12.5.5 Outsourced software development
12.6 TECHNICAL VULNERABILITY MANAGEMENT
12.6.1 Control of technical vulnerabilities
13 INFORMATION SECURITY INCIDENT MANAGEMENT
13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES
13.1.1 Reporting information security events
13.1.2 Reporting security weaknesses
13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS
13.2.1 Responsibilities and procedures
13.2.2 Learning from information security incidents
13.2.3 Collection of evidence
14 BUSINESS CONTINUITY MANAGEMENT
14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT
14.1.1 Including information security in the business continuity management process
14.1.2 Business continuity and risk assessment
14.1.3 Developing and implementing continuity plans including information security
14.1.4 Business continuity planning framework
14.1.5 Testing, maintaining and re-assessing business continuity plans
15 COMPLIANCE
15.1 COMPLIANCE WITH LEGAL REQUIREMENTS
15.1.1 Identification of applicable legislation
15.1.2 Intellectual property rights (IPR)
15.1.3 Protection of organizational records
15.1.4 Data protection and privacy of personal information
15.1.5 Prevention of misuse of information processing facilities
15.1.6 Regulation of cryptographic controls
15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE
15.2.1 Compliance with security policies and standards
15.2.2 Technical compliance checking
15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS
15.3.1 Information systems audit controls
15.3.2 Protection of information systems audit tools